INTERNATIONAL TELECOMMUNICATION UNION

Telecommunication
Development Bureau

T E L E F A X

Place des Nations
CH-1211 Geneva 20
Switzerland

Telephone +41 22 730 5111
Telefax Gr3: +41 22 733 7256
Gr4: +41 22 730 6500

Date: 9 octobre 2007 Page 1/9 Ref: DM-302

A : Etats Membres de l'UIT, Administrations/Régulateurs, Membres du Secteur, Membres associés, de la région Afrique

Fax: Voir liste annexée

Pour répondre:

Contact: Mme Margarida Evora Sagna
Bureau de zone de l'UIT pour l'Afrique de l'Ouest

E-mail: margarida.evora@itu.int

Fax: +221 8228013 Tel.: +221 849 77 20

M. Robert Shaw
Division applications TIC et cybersécurité
Politiques et stratégies

E-mail: cybmail@itu.int

Fax: +41 22 730 5484 Tel.: +41 22 730 5338

Objet: Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection de l'infrastructure de l'information critique, Praia, Cap-Vert, 27-29 November 2007

Madame, Monsieur,

Au nom de l'Union internationale des telecommunications (UIT), nous avons l'honneur de vous inviter à participer à l'Atelier pour l'**Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection de l'infrastructure de l'information critique (PIIC)**, qui se tiendra du 27 au 29 novembre 2007 à Praia, Ile de Santiago, République du Cap-Vert. Cet Atelier sera l'hôte du Ministère capverdien des transports et des infrastructures et sera organisé en coopération avec l'autorité de régulation du Cap-Vert, l'*Agência Nacional das Communicações (ANAC)*.

L'intégration des technologies de l'information et de la comunications dans la quasi-totalité des activités socio-économiques quotidiennes a accru la dépendance des personnes, des organisations et des Etats par rapport au maillage des réseaux mondiaux. La croissance rapide de l'utilisation des TIC ces dix dernières années et un nombre croissant d'incidents informatiques et d'activités frauduleuses ont conduit à un changement radical de la perception de l'importance que revêt la cybersécurité, évolution que n'a pas manqué de renforcer encore la prise de conscience croissante du lien étroit qui existe entre la cybersécurité et la PIIC.

Pour promouvoir la cybersécurité et protéger les infrastructures maillées critiques, il convient de prendre des mesures coordonnées au niveau des pays pour prévenir les incidents, réagir le cas échéant et rétablir la situation antérieure. Il faut disposer de cadres et de stratégies nationales pour permettre aux parties prenantes (personnes, organisations et Etats) de faire usage de tous les outils techniques, juridiquese et réglementaires disponibles pour encourager une culture de la cybersécurité, parallèlement à une coopération au plan régional et international. L'Atelier vise à réunir les représentants des Etats, les acteurs de l'industrie et d'autres groupes intéressés dans les pays de l'Afrique de l'Ouest afin qu'ils puissent discuter, partager des informations et collaborer à l'élaboration et à la mise en œuvre de cadre politiques, réglementaires et exécutoires nationaux pour la cybersécurité et la PIIC. Il intéressera:

- les spécialistes de l'information et de la communication des ministères et autres départements publics ;
- les institutions et départements chargés des politiques, de la législation et de l'exécution en matière de cybersécurité ; et
- les représentants des opérateurs, fabricants, fournisseurs de services, industriels et associations des consommateurs s'intéressant à la promotion d'une culture de la cybersécurité.

L'Atelier examinera en outre les initiatives susceptibles d'être prises au plan régional et international pour accroître la coopération et la coordination entre les différentes parties prenantes.

La participation à l'Atelier est ouverte aux Etats Membres de l'UIT, Membres de Secteur, Membres associés et autres parties prenantes intéressées, en particulier les représentants des organisations régionales ou internationales. Un nombre limité de bourses sera accordé à des participants de PMA. Pour obtenir une bourse, merci de retourner l'annexe 3 (Demande de bourse) à l'UIT Genève par fax: +41 22 730 5778.

L'Atelier se tiendra en anglais, français et portugais avec interprétation simultanée. Un projet d'ordre du jour est joint au présent courrier, et des informations complémentaires peuvent être consultées à www.itu.int/ITU-D/cyb/events/2007/praia/. Les contributions électroniques concernant les expériences au plan national seront les bienvenues.

Les participants ayant besoin d'assistance pour participer à l'Atelier sont priés de contacter Mme Anna Barboza par e-mail: anna.barboza@itu.int ou par fax: + 221 8228013. Le formulaire d'inscription doit être envoyé à Mme Anna Barboza au Bureau de zone de l'UIT, Dakar, Sénégal, avec copie à l'*Agência Nacional de Comunicações (ANAC)* ou par fax: +238 2613069, aussitôt que possible, mais au plus tard le 20 octobre 2007.

Nous nous réjouissons de votre participation active et de votre précieuse contribution.

Nous vous prions, Madame, Monsieur, de croire à l'assurance de notre haute considération.

Sami Al Basheer Al Morshid
Directeur

[original signé]

Pièces jointes:

- Projet d'ordre du jour (Annexe 1)
- Formulaire de pré-inscription (Annexe 2)
- Formulaire de demande de bourse (Annexe 3)
- Informations pratiques pour les participants à l'Atelier (Annexe 4) (disponible également en ligne à: www.itu.int/ITU-D/cyb/events/2007/praia/).

ANNEXE 1

Atelier de l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la protection de l'infrastructure de l'information critique

27-29 novembre 2007
Praia, Cap-Vert

Projet d'ordre du jour

Description: l'intégration des technologies de l'information et de la communication (TIC) dans la quasi-totalité des activités socio-économiques quotidiennes a accru la dépendance des personnese, des organisations et des Etats par rapport au maillage des réseaux mondiaux. La croissance rapide de l'utilisation des TIC ces dix dernières années et un nombre croissant d'incidents informatiques et d'activités frauduleuses ont conduit à un changement radical de la perception de l'importance que revêt la cybersécurité, évolution que n'a pas manqué de renforcer encore la prise de conscience croissante du lien étroit qui existe entre la cybersécurité et la protection de l'infrastructure de l'information critique (PIIC).

Pour promouvoir la cybersécurité et protéger les infrastructures maillées critiques, il convient de prendre des mesures coordonnées au niveau des pays pour prévenir les incidents, réagir le cas échéant et rétablir la situation antérieure. Il faut disposer de cadres et de stratégies nationales pour permettre aux parties prenantes (personnes, organisations et Etats) de faire usage de tous les outils techniques, juridiques et réglementaires disponibles pour encourager une culture de la cybersécurité, parallèlement à une coopération au plan régional et international. L'Atelier vise à réunir les représentants des Etats, les acteurs de l'industrie et d'autres groupes intéressés dans les pays de l'Afrique de l'Ouest afin qu'ils puissent discuter, partager des informations et collaborer à l'élaboration et à la mise en œuvre de cadres politiques, réglementaires et exécutoires nationaux pour la cybersécurité et la PIIC. Il intéressera:

- les spécialistes de l'information et de la communication des ministères et autres départements publics;
- les institutions et départements chargés des politiques, de la législation et de l'exécution en matière de cybersécurité ; et
- les représentants des opérateurs, fabricants, fournisseurs de services, industriels et associations des consommateurs s'intéressant à la promotion d'une culture de la cybersécurité.

L'Atelier examinera en outre les initiatives susceptibles d'être prises au plan régional et international pour accroître la coopération entre les différentes parties prenantes.

MARDI 27 NOVEMBRE 2007	
08:00–09:00	**Inscription**
09:00–10:15	**Ouverture de l'Atelier et mot de bienvenue**
	Allocution de bienvenue: Administration du Cap-Vert/Ministério das Infraestruturas e Transportes, Cap-Vert ***Remarques liminaires:*** Représentant de l'UIT-D
10:15–10:30	**Pause café/thé**
10:30–12:00	**Session 1: Elaborer une stratégie et créer un cadre national pour la cybersécurité et la protection de l'infrastructure de l'information critique (PIIC) – Présentation générale-**

	Description de la session: On est en général conscient de la nécessité d'entourer l'utilisation des TIC de confiance et de sûreté, en encourageant la cybersécurité et en protégeant les infrastructures critiques au niveau national. Comme les acteurs nationaux des secteurs public et privé apportent leur propre contribution à ces différentes questions d'importance, afin d'avoir une certaine cohérence, certains pays ont établi des cadres institutionnels en matière de cybersécurité/PIIC. La session 1 examinera, dans une perspective large, différentes façons de concevoir des cadres de ce type, ainsi que leurs éléments constitutifs, souvent similaires, afin de donner aux participants une idée générale des questions et enjeux.
12:00–13:30	**Déjeuner**
13:30–15:00	**Session 2: Elaboration d'une stratégie nationale pour la cybersécurité et la protection de l'infrastructure de l'information critique (PIIC)**
	Description de la session: De plus en plus les réseaux électroniques sont utilisés à des fins criminelles, ou pour des objectifs qui peuvent nuire à l'intégrité de l'infrastructure critique et créer des obstacles qui interdiront de profiter des avantages des TIC. Pour faire face à ses menaces et protéger les infrastructures, chaque pays doit disposer d'un programme d'action global abordant les questions techniques, juridiques et politiques, parallèlement à une coopération régionale et internationale. Quelles questions devaient être prises en considération dans le cadre d'une stratégie nationale pour la cybersécurité et la PIIC? Quels acteurs devraient être mis à contribution? Y a-t-il des exemples de cadres qui puissant être adoptés? La session 2 cherchera à approfondir divers modèles, examiner les meilleures pratiques et déterminer les principaux blocs constitutifs susceptibles d'aider les pays de l'Afrique de l'Ouest à établir des stratégies nationales pour la cybersécurité et la PIIC.
15:00–15:15	**Pause café/thé**
15:15–17:00	**Table ronde: Echanges d'informations sur un cadre pour la cybersécurité et la protection de l'infrastructure de l'information critique et l'élaboration d'une stratégie nationale**
17:00–17:15	**Synthèse de la journée et annonces**

MERCREDI 28 NOVEMBRE 2007	
09:00–10:15	**Session 3: Fondements juridiques et démarche réglementaire**
	Description de la session: Pour prévenir, détecter et contrer le cybercrime et le mauvais usage des TIC, il faut une législation appropriée, une coordination juridique au niveau international et des mesures exécutoires, ce qui suppose d'actualiser les dispositions, procédures et politiques du droit pénal pour faire face aux incidents de cybersécurité et contrer le cybercrime. En conséquence, de nombreux pays ont modifié leur code pénal, ou sont en train d'adopter des amendements, conformément aux conventions et recommandations internationales. La session 3 examinera divers modèles juridiques nationaux et déterminera les secteurs potentiels se prêtant à une coordination juridique internationale.
10:15–10:30	**Pause café/thé**
10:30–12:00	**Session 4: Fondements juridiques et démarche réglementaire (suite)**
	Description de la session: voir ci-dessus.
12:00–13:30	**Déjeuner**
13:30–15:00	**Session 5: Fondements juridiques et démarche réglementaire (suite)**
	Description de la session: voir ci-dessus.
15:00–15:15	**Pause café/thé**
15:15–17:00	**Table ronde: Echanges d'informations sur les fondements juridiques et la démarche réglementaire pour une cybersécurité améliorée.**
17:00–17:15	**Synthèse de la journée et annonces**

JEUDI 29 NOVEMBRE 2007	
09:00–10:15	**Session 6: Fonctions de surveillance, d'alerte et de réaction en matière d'incidents**
	Description de la session: Pour mettre en oeuvre un cybersécurité au niveau national, il faut impérativement se tenir prêt, détecter, gérer et réagir aux cyberincidents moyennant l'élaboration de fonctions de surveillance, d'alerte et de réaction en matière d'incidents. Pour une gestion efficace des incidents il faut tenir compte des aspects suivants : financement, ressources humaines, formation, capacités technologiques, relations entre services officiels et secteur privé et prescriptions juridiques. Une coopération à tous les niveaux de l'Etat, et avec le secteur privé, les universités, les organisations régionales ou internationales est indispensable pour sensibiliser aux attaques potentielles et aux ébauches de solutions. La session 6 examinera les meilleures pratiques en la matière ainsi que les normes connexes dans les domaines techniques, manageriel et financier liés à l'élaboration au niveau national ou régional de fonctions de surveillance, d'alerte et de réaction aux incidents.
10:15–10:30	**Pause café/thé**
10:30–12:00	**Session 7: Combattre les spasm et autres menaces connexes**
	Description de la session: Un des principaux risques pour la sécurité de l'Internet est constitué par le phénomène des spams, qui a évolué passant d'une gêne générale à une véritable menace pour la cybersécurité. Les spams sont maintenant le principal mécanisme de diffusion des virus qui peuvent bloquer des millions d'ordinateurs (par exemple botnets), ou pour lancer des attaques d'amorçage destinées à ferrer des informations financières soit privées, soit institutionnelles. Les spams servent également de plate forme pour de nombreux autres types de fraudes. Un certain nombre de contre mesures contre les spammeurs (techniques, financiers, formation des usagers) peuvent être utilisées, mais on constate un manque général de coordination au niveau international. La session 7 sera consacrée à certaines des normes, pratiques les meilleures et initiatives qui ont été lancées pour lutter contre le phénomène des spams et autres menaces connexes.
12:00–13:30	**Déjeuner**
13:30–14:45	**Session 8: Coopération régionale et internationale**
	Description de la session: une coopération régionale et internationale est extrêmement importante si on veut créer une culture de la sécurité, sans négliger le rôle des instances régionales pour faciliter les interactions et échanges. La session 8 explorera certaines des initiatives de coopération régionale et internationale en cours afin d'encourager les participants au séminaire à prendre part à d'autres actions concrètes qui pourraient être mises en œuvre dans la région de l'Afrique de l'Ouest, et au plan international.
14:45–15:00	**Pause café/thé**
15:00–16:00	**Session 9: Synthèse, recommandations et l'après**
	Description de la session: la dernière session du séminaire permettra de tirer les principales conclusions du débat. Elle sera consacrée à certaines initiatives de coopération régionale et internationale en cours destinées à encourager les participants au séminaire à prendre part à de futures actions concrètes qui pourraient être mises en œuvre dans la région et sur le plan international. Les recommandations qui seront élaborées au terme de la session 9 viseront à établir la direction des futures activités pour améliorer la cybersécurité et accroître la protection des infrastructures d'information critique dans la région.
16:00–16:15	**Clôture du séminaire**
	Remarques de clôture: Administration du Cap-Vert/ Ministério das Infraestruturas e Transportes, Cape Verde ***Remarque de clôture:*** Représentant de l'UIT-D

ANNEXE 2

Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la PIIC

Praia, Cap-Vert, 27 – 29 Novembre 2007

FORMULAIRE DE PRÉINSCRIPTION

Formulaire à retourner à
Bureau de zone de l'UIT pour l'Afrique de l'Ouest, Dakar, Sénégal par email: anna.barboza@itu.int
ou par fax: + 221 822 80 13
avec copie à l' ANAC, Cap-Vert par fax: +238 261 30 69, avant le **20 octobre 2007**

1. M./ Mme
_____
(nom de famille) (prénom)

2. Titre officiel: _____

3. Organisation: _____

4. Adresse: _____

5. Pays: _____ **Nationalité:** _____

6. TEL: _____ **FAX:** _____ **E-MAIL:** _____

7. N° Passport: _____ **Délivré à:** _____

8. Date de délivrance: _____ **Date d'expiration:** _____

9. Date de naissance: _____ **Lieu de naissance:** _____

10. Lieu de délivrance du visa: _____
(dans votre pays, ou un autre pays sur le trajet)

11. Relation avec l'UIT
- ☐ Administration d'un Etat Membre de l'UIT
- ☐ Membre de Secteur de l'UIT
- ☐ Membre associé de l'UIT
- ☐ Non-Membre

RENSEIGNEMENTS CONCERNANT VOTRE VOL

Date d'arrivée	Heure d'arrivée	Numéro de vol
Date de départ	Heure de départ	Numéro de vol

RESERVATION D'HOTEL

Nom de l'hôtel:……

☐ Chambre simple ☐ Chambre double
☐ Suite simple ☐ Suite double

Date d'entrée: _____ Date de départ: _____

Date: _____	Signature:

ANNEXE 3

Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la PIIC
Praia, Cap-Vert, 27 – 29 Novembre 2007

Ministério das Infraestruturas e Transportes

FORMULAIRE DE DEMANDE DE BOURSE

Prière de renvoyer à: Chef du Service des bourses
UIT, Place des Nations
CH - 1211 Genève 20, Switzerland

Tel.: +41 22 730 5487
Fax: +41 22 730 5778
christine.jouvenet@itu.int

LES CANDIDATURES FEMINIES SONT ENCOURAGEES

DEMANDE DE BOURSE COMPLETE A SOUMETTRE AVANT LE 20 octobre 2007
(Prière de dactylographier/écrire lisiblement)

Pays _____Administration /Organisation _____

Nom de famille M./Mme_____ Patronyme _____

Fonction actuelle (titre): _____

Adresse postale professionnelle: _____

_____

Téléphone: _____ Fax: _____

E-mail (écrire lisiblement)_____

DONNEES PERSONNELLES DU CANDIDAT:

PASSPORT:

Lieu et place de naissance: _____

Nationalité _____ Numéro du passeport _____

Date de délivrance du passeport _____ Lieu de délivrance _____

Date d'expiration _____

CONDITIONS: Les bourses sont attribuées aux conditions suivantes:

1. Une bourse par pays éligible.
2. Bourse complète pour PMAs et partielle (indemnité journalière de subsistance uniquement) pour les autres pays éligibles.
3. Une indemnité journalière pour couvrir les dépenses de logement et frais divers.
4. Il est impératif que les participants auxquels sont attribués des bourses de l'UIT soient présents depuis le premier jour et participant pendant toute la durée couverte par la bourse.

Lieu, date et signature du candidat _____

POUR QU'UNE DEMANDE DE BOURSE SOIT VALIDEE, IL FAUT QUE SOIENT APPOSES CI-DESSOUS LE NOM ET LA SIGNATURE DU REPRESENTANT DE L'ADMINISTRATION RESPONSABLE, AVEC LE CACHET CORRESPONDANT:

Nom et titre du responsable en lettres majuscules: _____

Signature du responsable certificateur: _____ **Date:** _____

ANNEXE 4

INFORMATIONS PRATIQUES POUR LES PARTICIPANTS AU SEMINAIRE

Atelier pour l'Afrique de l'Ouest sur les cadres politiques et réglementaires pour la cybersécurité et la PIIC

Ministério das Infraestruturas e Transportes

Praia, Cap-Vert, 27 - 29 novembre 2007

1 Lieu

L'Atelier aura lieu au **Praia Mar Hotel**

Adresse: Praia Mar Hotel
CP 75 Prainha
Praia – SANTIAGO
CAP-VERT

Tel: +238 261 37 77
Fax:+238 261 29 72

E-mail: praiamar@cvtelecom.cv

2 Pour arriver à Praia, Cap-Vert

Il existe des vols directs réguliers depuis Dakar, Lisbonne, Paris, et des vols moins fréquents depuis d'autres villes d'Europe ou d'Afrique à destination de Praia, Cap-Vert.

3 Arrivée et transports locaux

Prière de noter que les participants à l'Atelier doivent prendre leurs propres dispositions pour se transporter de l'aéroport à leurs hôtels respectifs, dont certains assurent des services de navettes.

4 Prescriptions d'entrée au Cap-Vert

Pour entrer au Cap-Vert il faut disposer d'un passeport valuable et d'un visa. Sont exemptés les ressortissants des pays de la CEDEAO. Les participants sont donc invités à contacter l'ambassade du Cap-Vert dans leurs pays d'origine pour obtenir le visa nécessaire. En cas de difficultés pour obtenir ce visa, les participants voudront bien contacter l'Agencia Nacional das Communicaçoes (ANAC), Tél.: +238 260 44 00, ou fax +238 2613069.

4 Monnaie

La monnaie du Cap-Vert est l'Escudos. Le taux de change actuel est de 1 EURO = 110 escudos ou 1 USD = 80 escudos. L'argent peut être change dans les banques et les bureaux de change.

5 Electricité

Le secteur est de 220 volts / 50 Hz. Pour une tension plus basse, s'adresser à la réception de l'hôtel.

6 Climat

Le Cap-Vert se situe en Afrique de l'Ouest (au Nord de la zone tropicale). Le séminaire aura lieu pendant la saison sèche, lorsque la température est d'environ 24°C et l'humidité faible.

7 Santé et vaccinations

Un certificat de vaccination internationale est nécessaire pour la fièvre jaune.

8 Contact

Pour toute autre information, prière de contacter:

Mme Manuela Pereira

Tél.: +238 2604400

Fax: +238 2613069

E-mail: manuela.pereira@anac.cv

9 Logement

Des hôtels offrant des tarifs préférentiels sont recommandés dans la liste ci-dessous :

LISTE D'HOTELS ET DE RESIDENCE RECOMMANDES

HOTEL	CHAMBRE SIMPLE		CHAMBRE DOUBLE		TELEPHONE	FAX	EMAIL
	ESCUDOS	EUROS	ESCUDOS	EUROS			
Hotel Praia Mar **** (lieu du séminaire)	11.250	102	14.110	128	+238 260 84 40	+238 261 29 72	praiamar@cvtelecom.cv
Hotel Tropico ****	10.900	99	13.790	122	+238 261 42 00	+238 261 52 25	hotel.tropico@cvtelecom.cv
Pérola ***	4.455	42	5.850	55	+238 260 14 40	+238 261 14 48	perola@cvtelecom.cv
Eurolines ***	3.500	30	-	-	+238 260 30 10	+238 261 66 60	Eurolines@cvtelecom.cv
Residencial Praia-Maria ***	4.770	46	5.600	57	+238 26175 23	+238 261 85 54	res.praiamaria@cvtelecom.cv
Residencial Bera Mar***	4.950	45	6.930	63	+238 261 64 00	+238 261 30 69	beramar@cvtelecom.cv