



Atelier sur l'harmonisation du cadre légal pour la cybersécurité en Afrique du Nord

Rabat, Maroc, 27-28 Juillet 2010

Aide mémoire

Les sociétés de la région d'Afrique, à l'instar des sociétés dans d'autres parties du monde, qui dépendent de plus en plus des technologies d'information et de communication sont donc vulnérables à des menaces telles que le cyber crime.

Les criminels tels que les pirates, les groupes du crime organisé et les terroristes voient en le potentiel des TIC un moyen pour faciliter leurs crimes. Pendant ce temps, les consommateurs hésitent à transmettre des données à caractère personnel et de cartes de crédit sur Internet, la sécurité et la confidentialité étant leur préoccupation numéro un. Par ailleurs les entreprises doivent faire face à des pertes importantes de données de propriété industrielle, propriété intellectuelle, et l'accès en ligne aux clients et fournisseurs en raison de violations de la sécurité.

En l'absence des lois pénales et règlements, ainsi que la capacité d'enquêter pour l'application de ces lois à l'échelle nationale, et à coopérer au niveau international, les économies peuvent devenir attractives comme des paradis pour les mauvais acteurs, des référentiels de données criminelles, et des centres de blanchissement d'argent et des activités terroristes.

Pour que les TIC puissent contribuer à la croissance économique, au développement humain, et à la démocratisation, ils doivent être fiables et sécurisés. Un manque de confiance et de sécurité met en péril de nombreux développements qui pourraient être soutenues par une économie de la connaissance et de la société largement accessibles et de confiance.

- La croissance du e-commerce - entre les entreprises et entre entreprises et consommateurs.
- L'attraction des investissements étrangers nécessaires à la création d'entreprises, la modernisation des infrastructures, et de l'innovation - les capitaux ne vont pas vers les pays dont le système juridique ne répond pas aux questions de sécurité informatique.
- E-gouvernement - des efforts pour rendre le gouvernement plus adapté et accessible sont menacées par des problèmes de sécurité et de crainte d'abus.
- Création d'emplois grâce au développement des «services de back-office» - les entreprises mondiales qui cherchent des coûts salariaux plus bas pour la saisie des données et "arrière-salle" les activités de traitement de données ne vont pas envoyer leurs données vers des pays où la loi laisse sans protection.
- La fiabilité des infrastructures essentielles - même dans les pays en développement, la production d'électricité et la distribution, transports, banques, gouvernement, et les opérations de soins de santé sont de plus en plus tributaires des systèmes d'information
- Protection de la vie privée et des données de propriété - les communications et les données stockées des entreprises et les particuliers doivent être protégées contre les interceptions illégales, d'accès et surveillance du gouvernement arbitraire.
- le développement de la télémédecine et les centres de soins de santé - les populations mal desservies n'auront pas confiance à leurs renseignements médicaux dans un environnement à moyens de communication insécurisée.
- L'utilisation des technologies de l'information pour l'enseignement à distance - services de l'emploi, l'amélioration des compétences des travailleurs, et le développement des petites et moyennes entreprises.

La Commission économique des Nations Unies pour l'Afrique (CEA) a reconnu la nécessité de relever ce défi au niveau national, sous-régional et régional. Dans ce contexte, le Bureau pour l'Afrique du nord et la Division des TIC, de la science et de la technologie de la CEA, en collaboration avec le Conseil de l'Europe et Microsoft se sont associés pour organiser un atelier sur l'harmonisation de la législation pour la cybersécurité en Afrique du Nord. Cet événement comprendra une analyse des Cyber législations en vigueur dans les pays d'Afrique du Nord et en identifier les besoins de réforme.

L'atelier permettra le partage d'expériences en termes de mesures prises dans différents pays, à fournir un soutien et des conseils pour les réformes en cours et pour discuter d'un plan d'actions et de mesures visant à compléter la législation par la formation et la coopération avec les fournisseurs de services.

L'atelier se concentrera sur l'harmonisation de la législation sur la cybercriminalité, comme élément de l'ordre du jour de cybersécurité, et l'effort mondial pour établir la confiance et la sécurité dans l'économie du savoir et de la société.

Objectifs

L'objectif de cet atelier est de soutenir le renforcement et l'harmonisation des législations sur la cybercriminalité dans les pays d'Afrique du Nord, conformément aux normes internationales.

Les ateliers proposés pourront améliorer les connaissances des participants par les mesures législatives nécessaires pour lutter contre les crimes impliquant des ordinateurs et l'Internet. Les participants évalueront l'état actuel de leur droit de fond et de procédures, discuter de l'élaboration (ou le perfectionnement) d'un cadre légal pour les enquêtes et les poursuites de la cybercriminalité.

L'atelier aidera les pays d'Afrique du Nord à respecter leurs engagements au Sommet Mondial sur la Société de l'Information à s'efforcer d'adopter des cadres légaux de lutte contre la cybercriminalité, de renforcer la cybersécurité et d'identifier ou développer des unités de répression de la cybercriminalité, capable de fournir une assistance internationale.

À la fin de l'atelier, les participants doivent:

- avoir une meilleure compréhension sur la façon de formuler des projets de loi sur la cybercriminalité;
- avoir procédé à une analyse de législations nationales sur la cybercriminalité, comme en témoignent les profils de pays mis à jour;
- avoir identifié les mesures à prendre pour renforcer leur législation nationale;
- se familiariser avec les bonnes pratiques concernant la coopération entre les services répressifs et avec les fournisseurs de services Internet, qui peuvent aussi être utiles pour les pays d'Afrique du Nord; et
- se familiariser avec des concepts pour la formation des forces de l'ordre, des procureurs et des juges en matière de cybercriminalité et de preuve électronique.
- un plan d'action concerté pour la mise en œuvre d'une législation harmonisée du cyber espace dans les pays participants d'Afrique du nord.

Participants

Les délégations comprennent des experts en cybercriminalité provenant des départements d'application des lois, des ministères de la justice, et des décideurs politiques, y compris des experts des organes législatifs, des tribunaux et des universités. Ils bénéficieront directement des informations et d'une aide précieuse dans le développement (ou le perfectionnement) des cadres légaux.

Contenu de l'atelier

Cet atelier de 2 jours va aborder les points suivants:

- Aperçu des menaces émergentes et tendances dans des activités criminelles liées aux TIC;
- Discussion de la cybercriminalité et les efforts multilatéraux existants de la cybersécurité et la façon dont ce travail peut être utilisé pour atteindre les objectifs des pays;
- Discussion de la législation nécessaire pour la collecte et l'utilisation de la preuve électronique, ainsi que pour améliorer la coopération internationale en matière de cybercriminalité;
- Comparaison des lois en vigueur des pays d'Afrique du Nord avec la Convention sur la cybercriminalité;

- Discussion des efforts antérieurs des pays visant à élaborer des cadres approfondies et des expériences avec le langage légal particulier;
- Examen, discussion et raffinement de la législation existante et le projet de voie à l'harmonisation;
- Discussion et proposition d'un plan d'action pour l'harmonisation de la législation cyber en Afrique du Nord.

Langue de travail

Les travaux de l'atelier seront en français.

Lieu et date

Rabat, Maroc, 27-28 Juillet 2010.

Contacts:

Monsieur Mohamed Timoulali
Conseiller régional
Bureau de la CEA pour l'Afrique du nord
Tél + (212) 537 71 78 29
Fax + (212) 537 71 27 02
E-mail mohamedt@uneca.org