Sommet Connecter le monde arabe
5-7 mars 2012
Doha, Qatar

15 février 2012
Original: anglais

Utilisation des TIC: renforcer la confiance et la sécurité

Document d'information

1 CONSIDÉRATIONS GÉNÉRALES

Le Sommet mondial sur la société de l'information (SMSI) a reconnu les risques réels et non négligeables posés par un défaut de confiance et de sécurité dans l'utilisation des TIC et par la prolifération de la cybercriminalité. Les paragraphes 108 à 110 de l'Agenda de Tunis pour la société de l'information, annexe comprise, définissent un programme de mise en oeuvre multi-parties prenantes, au niveau international, du Plan d'action du SMSI, qui reprend les onze grandes orientations du Plan d'action et désigne des coordonnateurs pour chacune d'entre elles. Au cours du Sommet, les gouvernements et les dirigeants internationaux ont désigné l'UIT comme coordonnateur de la mise en oeuvre de la grande orientation C5 du Sommet, "Etablir la confiance et la sécurité dans l'utilisation des TIC".

Dans le monde moderne, les TIC interviennent dans tout ce que nous faisons et leur rôle ne va cesser de croître pour accompagner le développement socio-économique. Elles ont amélioré l'efficacité des entreprises, de la gouvernance, de l'enseignement, de la santé, de l'environnement et de la communication. La révolution numérique a modifié le mode de fonctionnement des affaires et des gouvernements. La mondialisation et le progrès technologique ont rendu les principales infrastructures vulnérables et les ont converties en cibles éventuelles du terrorisme. Les pays sont confrontés à des risques réels et leurs adversaires pourraient tirer parti de la vulnérabilité des systèmes d'information cruciaux. En effet, ils cherchent à neutraliser les infrastructures essentielles et les principales ressources pour menacer la sécurité nationale, provoquant des dégâts considérables, pour affaiblir l'économie mondiale et pour porter atteinte au moral et à la confiance du public. Actuellement, le cyberespace est loin d'être sûr. Au vu de cet environnement en pleine évolution, il existe un besoin urgent de prendre des mesures, au niveau national comme au niveau international, contre la cybercriminalité sous toutes ses formes.

Ces dernières années, les pays du monde arabe ont accompli des progrès considérables dans les domaines des technologies de l'information et de la communication et concernant les variables utilisées par les personnes, les entreprises et les gouvernements pour évaluer le stade actuel de développement et les répercussions des stratégies nationales et régionales en matière de TIC. Ces Etats manifestent un vif intérêt, par exemple, pour les initiatives en matière de technologies et en tirent des bénéfices croissants, en créant des opportunités de recherche et développement, en intensifiant la diffusion des technologies ou en favorisant l'environnement socioéconomique par la création de nouvelles perspectives d'emploi.

Compte tenu de ce changement radical, les représentants du monde arabe ont reconnu le besoin d'encourager les activités liées à la cybersécurité, dans le cadre des stratégies nationales et régionales, afin de mieux réagir aux cyberattaques. Bien que les Etats du monde arabe assurent la promotion des TIC et aient mis en place des mesures à suivre pour utiliser ces technologies en toute sécurité, bien souvent, leurs démarches sont parcellaires et entrent en concurrence les unes avec les autres. Par conséquent, une coordination et une harmonisation des mesures et des cadres législatifs sont nécessaires pour que la région parle d'une seule voix et soit prête à se défendre des cyberattaques.

2 OBJECTIFS DU PRÉSENT DOCUMENT

Le monde arabe est confronté à plusieurs difficultés dans sa lutte contre les cybermenaces et la mise en oeuvre des cadres législatifs adaptés et des infrastructures nationales appropriées pour lutter efficacement contre ces cybermenaces. Le présent document identifie plusieurs défis à relever par ces nations pour améliorer la cybersécurité tout en se dotant des infrastructures adéquates pour protéger les données critiques. Il vise à évaluer les mesures adoptées par les pays participants dans leur lutte contre les menaces de la cybercriminalité. Il conclut, enfin, par une série de recommandations concrètes à l'attention des partenaires au développement et des gouvernements, concernant notamment l'application de programmes exhaustifs de renforcement des capacités, la mise en place d'équipes nationales d'intervention en cas d'urgence informatique et la coordination à l'échelle régionale.

3 RÉSUMÉ DE LA SITUATION ACTUELLE

Les Etats Membres de la Ligue arabe présentent des situations très diverses en termes de législation en vigueur concernant la cybercriminalité, de mise en place de centres nationaux chargés de résoudre les problèmes en matière de sécurité et capables de remédier aux incidents les plus graves, et de mesures concrètes de protection en ligne des enfants.

3.1 Politiques et cadres réglementaires, aux niveaux national et régional, pour garantir la confidentialité des données et lutter contre la cybercriminalité

La plupart des gouvernements ont ébauché relativement récemment des cadres législatifs de lutte contre la cybercriminalité. Cependant, ces dispositions législatives portent sur des cybermenaces précises et concernent surtout le commerce électronique, alors que ces dernières années, malheureusement, les cybermenaces envahissent plusieurs autres domaines. Par conséquent, une approche globale est nécessaire pour les déjouer.

D'autres pays doivent commencer par élaborer des règles de fond et par se coordonner avec les agences nationales en charge de la sécurité et des activités en ligne. Dans certains d'entre eux, aucune loi globale sur la cybersécurité n'a encore été promulguée ou adoptée. La criminalité appliquée aux TIC est généralement sanctionnée suivant les codes pénaux en vigueur, qui sont rarement actualisés ou adaptés aux tendances mondiales. Un vide légal est apparu dans le domaine de la cybercriminalité, obligeant le législateur à intervenir pour promulguer des textes juridiques nationaux garantissant que les activités rendues possibles par les nouvelles technologies puissent être érigées en crimes ou délits, à la lumière des textes traditionnels devenus obsolètes pour être appliqués dans le domaine des TIC. Comme il l'a été remarqué, d'après les normes internationales, la législation devrait traiter de domaines tels que:
i) l'incrimination; ii) les mesures relatives à la procédure; iii) les éléments de preuve électroniques; iv) la compétence des juridictions; v) la responsabilité des fournisseurs d'accès Internet; vi) la coopération internationale.

La coopération régionale entre les pays du monde arabe est primordiale pour lutter contre cette criminalité, car celle-ci émane de différents endroits et s'appuie sur des techniques modernes. La région a éperdument besoin de consolider ses mécanismes de coopération pour lutter contre ces types d'infractions qui l'envahissent déjà, en l'absence de toute législation spécifique qui s'y oppose. De sérieux efforts sont toutefois déployés pour adopter une convention spéciale sur la coopération régionale dans le monde arabe, afin de lutter contre la criminalité informatique ou cybercriminalité, qui reste pour l'instant à l'état de projet; en outre, une loi-cadre pour les pays arabes sur la lutte contre la criminalité liée aux technologies de l'information a également été adoptée.

Enfin, l'intégration des normes internationales aux systèmes juridiques nationaux est importante (certains pays pouvant considérer que des infractions reconnues ailleurs n'en sont pas chez eux) pour favoriser la coopération internationale (de manière à ce que tous les pays définissent les infractions de la même manière) et éviter que des pays n'en arrivent à jouer, de fait, le rôle de refuges dans la région.

3.2 Création des équipes d'intervention en cas d'incident lié à la sécurité informatique (CSIRT)/des équipes d'intervention en cas d'urgence informatique (CERT), à l'échelle nationale, et coordination entre elles

Malheureusement, seuls quelques Etats Membres de la Ligue arabe ont instauré des centres nationaux de lutte contre les cyberattaques. Par conséquent, il est difficile de réagir efficacement à l'une de ces cyberattaques et de réparer les dégâts causés. Pour ce faire, une assistance est nécessaire et une coordination doit être mise en oeuvre entre les membres de la Ligue arabe.

En particulier, huit pays sur les 22 ont mis en place des équipes nationales d'intervention en cas d'urgence informatique (notamment Oman, l'Arabie saoudite et la Tunisie), mais tous ne se sont pas coordonnés à l'échelle régionale. Pour certains d'entre eux, tels que l'Egypte, le Maroc et le Qatar, la création d'une équipe CERT nationale était une priorité du gouvernement pour mettre en oeuvre une approche globale de la cybersécurité, faisant intervenir la législation, le renforcement des capacités et les infrastructures. Pour d'autres pays de la région, en revanche, la mise en oeuvre d'une Equipe d'intervention en cas d'urgence informatique est toujours à l'ordre du jour ou a démarré lentement, après la mise en place d'un cadre législatif et réglementaire.

A travers deux importantes initiatives régionales, certains pays ayant déjà créé leur équipe CERT nationale ont décidé de se coordonner dans le but de construire un cyberespace sûr, simple et tranquille pour leurs citoyens. L'Equipe nationale d'intervention en cas d'urgence informatique du Conseil de coopération du Golfe (GCC-CERT)[1], par exemple, a établi une coopération régionale entre les Etats du Golfe (Oman, les Emirats arabes unis, le Qatar, le Koweït, l'Arabie saoudite et Bahreïn) autour de la sécurité de l'information. Elle vise à échanger des points de vue et des bonnes pratiques et à donner des recommandations sur des sujets liés au cyberespace.

Reconnaissant par ailleurs l'existence de menaces dans le cyberespace, l'Organisation de la coopération islamique (OCI) a décidé de la création d'un instrument de coopération entre les équipes CSIRT et CERT de ses Etats membres, l'OIC-CERT. A l'heure actuelle, 18 pays membres de l'OCI en font partie et diverses activités sont menées dans le but de favoriser le développement des capacités des équipes CERT et l'échange d'informations concernant les points de vue et les sujets liés à la cybersécurité. L'OIC-CERT a instauré de nombreuses initiatives de coopération et de nombreux partenariats entre les équipes CERT de la région afin d'y renforcer la cybersécurité.

3.3 Protection des enfants et des jeunes des pays arabes contre les contenus dangereux sur Internet

Certains pays s'occupent activement des questions relatives à la protection en ligne des enfants et ont mis en place des activités destinées à promouvoir la sécurité en ligne à l'échelle nationale. Ces pays ont instauré un comité ou un groupe de travail interinstitutionnel, formé des différents groupes de parties prenantes, à savoir, le gouvernement, l'industrie, les professions juridiques, les ONG concernées, les associations de protection de l'enfance et les universités, afin de veiller à la mise en oeuvre de la stratégie nationale de protection en ligne des enfants. Dans certains pays, l'équipe CERT nationale a pour tâche de diriger la stratégie nationale destinée à promouvoir la culture de la sécurité des TIC dans la société, à introduire des normes de sécurité sur Internet, à sensibiliser à la déontologie de l'utilisation envisagée des TIC pour les enfants, etc.

---

[1] http://www.itu.int/ITU-D/cyb/events/2008/brisbane/docs/lewis-Q-CERT-incident-management-brisbane-july-08.pdf (en anglais)

D'autres pays de la région doivent toutefois encore étoffer leur stratégie nationale relative à la protection en ligne des enfants, notamment à travers des mesures préventives, des normes communes, la législation ou la sensibilisation de l'opinion publique. En particulier, une coopération régionale et internationale est nécessaire pour faire partager les expériences de chacun et améliorer la manière de protéger les enfants sur Internet.

4 ENJEUX ET PERSPECTIVES

Les Etats Membres de la Ligue arabe sont confrontés à plusieurs enjeux liés à différents aspects, notamment l'environnement législatif, la sensibilisation des utilisateurs et les infrastructures nationales.

En contrepartie de l'effet positif des TIC, le secteur privé, les organisations internationales et les gouvernements offrent des solutions et des réponses mondiales aux cybermenaces d'envergure internationale. Néanmoins, à l'échelle nationale, les pays doivent renforcer leurs compétences (en matière de ressources humaines, d'infrastructures et de législation) afin d'améliorer leurs aptitudes de lutte contre la cybercriminalité.

- Les secteurs liés aux TIC ont besoin d’un marché international dynamique et encourageant pour s’épanouir, à condition qu’existe un cadre législatif fiable pour réguler l’utilisation des TIC et, si besoin, sévir efficacement en cas de non-respect, et une approche globale s’attachant à la coopération entre le secteur privé et le gouvernement et à l’organisation d’activités de sensibilisation et de prévention. Les gouvernements, le secteur privé et les ONG doivent coordonner leurs efforts et travailler ensemble à la création d’un tel environnement. La plupart des pays développés, ainsi que certains pays en développement, ont déjà mis à jour leur cadre juridique et réglementaire pour l’adapter aux besoins créés par les nouvelles technologies, mais les bases d’un environnement favorable dépendent également de la formation de directives régionales promouvant l’harmonisation de la législation et de la réglementation en matière de TIC, car elle facilite et accélère l’utilisation de leurs applications. De ce point de vue, la plupart des Etats arabes ont mis en place des cadres réglementaires qui ne luttent pas nécessairement contre les cybermenaces mondiales ni ne sont harmonisés au niveau régional.
- Les lourds investissements réalisés ces dernières années par les nations arabes dans les domaines de la recherche, de l'éducation et des TIC illustrent leur engagement en faveur d'une transition vers une économie du savoir. Une économie qui dépend de l'utilisation stratégique et généralisée des TIC requiert, par défaut, la maîtrise des TIC et la confiance en leur utilisation. Ces deux caractéristiques supposent le besoin de renforcer une double capacité - savoir et pouvoir utiliser les TIC, d'une part, et pouvoir, à moyen terme, les généraliser, innover et se les approprier, d'autre part - et la transition, à long terme, vers la culture de l'aisance et de la confiance. Or, les Etats arabes n'investissent pas suffisamment dans le renforcement des capacités pour sensibiliser l'opinion publique aux cybermenaces à travers des programmes éducatifs – à savoir, la prise de conscience de l'ampleur de l'utilisation et des retombées de l'application des TIC ainsi que des menaces qui y sont liées – et pour favoriser et promouvoir les instruments et les actions permettant d'améliorer la sécurité sur Internet.
- Si certains Etats arabes ont certes inclus des programmes en matière de cybersécurité à leur programme national, cela ne signifie pas nécessairement qu'ils investissent dans la création d'infrastructures nationales capables d'aider les autorités du gouvernement ou les habitants locaux à réagir en cas de cybermenaces. Peu de programmes d'investissement visent à financer la création ou la croissance de composants stratégiques des infrastructures nationales. Dès lors, des mécanismes financiers destinés à garantir la réalisation d'investissements en faveur de la sécurité dans le cyberespace doivent être définis et adoptés, dans le cadre de la transition d'une stratégie traditionnellement réactive à une stratégie progressivement préventive.

La complexité de ces enjeux demande des approches transversales, sous la forme de processus multi-parties prenantes, d'une part, et d'une collaboration interservices accrue entre les différentes autorités concernées, d'autre part. La Ligue des Etats arabes pourrait fournir le cadre adéquat pour une approche harmonisée, par les Etats arabes membres, d'un cyberespace plus sûr, en termes de législation et d'investissement financier, et pour créer une stratégie régionale de cyberdéfense afin de lutter contre la cybercriminalité. Par ailleurs, les Etats arabes ayant des aspects culturels et religieux en commun, ils sont en mesure de créer, au niveau régional, des instruments tels que la mise en place de programmes éducatifs, la participation du secteur privé et la coopération avec des organisations locales. Certaines initiatives régionales déjà en place, comme l'OIC-CERT ou le GCC-CERT, pourraient contribuer à stimuler la création d'autres équipes CERT nationales et la coordination entre elles.

5 CONCLUSIONS ET RECOMMANDATIONS

D'après les points mis en évidence dans le présent rapport et d'après l'objectif du sommet Connecter le monde arabe, des mesures rapides sont nécessaires pour les pays dépourvus de stratégie nationale axée sur le renforcement des infrastructures en matière de cybersécurité. Quant aux pays ayant déjà une structure élaborée au niveau national et au niveau régional, ils ont besoin de renforcer leur coopération et leur collaboration pour créer une stratégie régionale harmonisée en matière de cybersécurité.

5.1 Cadre législatif et structures d'organisation:

1) Au niveau gouvernemental et ministériel, les décideurs doivent prendre en considération la sécurité, la fiabilité et la disponibilité des systèmes de tous les projets en cours relatifs aux infrastructures des TIC et leur attribuer une priorité suffisamment élevée. Le principe de défense en profondeur devrait également être adopté par les gouvernements dans tous les projets liés aux TIC.

2) Les parties prenantes devraient accélérer le processus de modification ou d'adoption de la législation relative à Internet afin de garantir la cohérence des cadres juridiques avec les différentes normes nationales relatives à l'incrimination, aux mesures en matière de procédure, aux éléments de preuve électroniques, à la compétence des juridictions et à la responsabilité des fournisseurs d'accès Internet. Un tel cadre juridique devrait permettre non seulement de traiter des aspects nationaux, mais aussi de faciliter la coopération internationale.

3) Les Etats Membres de la Ligue arabe devraient solliciter une assistance technique lorsqu'ils en ont besoin afin d'accélérer l'examen en profondeur de la législation et sa modification si nécessaire.

4) Il est important de concevoir et de mettre en oeuvre des campagnes de sensibilisation pour éduquer les utilisateurs, les responsables de l'application des lois et les dirigeants à la législation relative à Internet, aux conséquences de la cybercriminalité et aux mesures pour lutter contre elle. Les équipes nationales CSIRT/CERT peuvent assumer le rôle prépondérant de créer des campagnes de sensibilisation à la cybersécurité.

5) Les responsables politiques devraient sensibiliser l'opinion publique aux risques du progrès technologique pour le marché et les consommateurs et envisager des mesures réglementaires pour s'attaquer à des questions telles que la protection des données à caractère personnel, la protection des mineurs et la protection des utilisateurs vis-à-vis des logiciels malveillants.

6) A l'heure actuelle, l'une des mesures les plus urgentes est la création d'équipes CSIRT/CERT nationales et l'acquisition du savoir-faire technique nécessaire à leur fonctionnement. A cet effet, on peut tirer parti de l'expérience acquise par les Etats Membres arabes qui ont créé leurs propres équipes CSIRT/CERT, en complément de l'expérience de l'UIT, en ce qui concerne l'aide aux Etats Membres.

7) Pour diffuser la culture de la cybersécurité, les parties prenantes peuvent également entreprendre des activités telles que des programmes de recherche en rapport avec des domaines liés à la cybersécurité pour des étudiants de l'enseignement supérieur. Ces programmes de recherche peuvent être associés à des avantages, tels qu'une bourse ou un emploi, afin d'encourager la participation.

5.2 Renforcement des capacités

La formation d'une culture de la cybersécurité a plusieurs implications, qui s'étendent à tous les secteurs: stratégies et politiques en matière de sécurité, cadre et réglementation juridiques, systèmes et procédés, technologies et outils, compétences et sensibilisation, coopération et réseaux. En outre, une gestion efficace du changement demande qu'une évolution généralisée comme celle-ci s'accompagne d'une stratégie globale de renforcement des capacités humaines et institutionnelles, qui se composerait essentiellement d'un programme d'amélioration de la sensibilisation, d'éducation et de formation, afin de consolider les compétences appropriées pour réaliser une transition progressive vers la "nouvelle" culture.

Ces aspects sont les suivants:

1) programme de renforcement de la sensibilisation de toute la population concernée, comportant des messages ciblés et des méthodes de diffusion;

2) utilisation de l'informatique et des TIC à tous les niveaux de l'enseignement scolaire;

3) programme commun d'enseignement de la cybersécurité dans les établissements d'enseignement supérieur;

4) programmes spécifiques d'études élaborés séparément, pour les responsables politiques, les services juridiques et les services de police, accompagnés d'un programme de mise en oeuvre du renforcement des capacités visées comportant des bonnes pratiques, des outils/laboratoires et des ateliers;

5) encouragement des instituts de recherche à étudier ce sujet, au moyen de bourses spéciales et de mécanismes d'attribution de primes;

6) sélection, par les universités locales et régionales et les instituts de recherche, d'instituts spécialisés externes comme partenaires ou comme établissements fournissant une opportunité de parrainage ou de stage;

7) renforcement de forums et d'organes régionaux pour échanger et partager des informations, des incidences, des bonnes pratiques et des expériences;

8) élaboration de directives, d'outils de planification et de manuels sur les aspects de la technologie ou de la politique en matière de cybersécurité;

9) élaboration de kits pratiques sur la cybersécurité locale à l'attention des responsables politiques et des autres secteurs concernés;

10) élaboration de matériel de formation sur les stratégies en matière de technologies et sur l'évolution de ces dernières pour la mise en oeuvre de la cybersécurité;

11) organisation d'ateliers, de réunions et de séminaires pour aborder les aspects techniques, politiques, juridiques et stratégiques de la cybersécurité;

12) assistance à la conception de lois et d'une législation-type pour la prévention en matière de cybersécurité;

13) identification des exigences de la cybersécurité et proposition de solutions pour le développement d'applications sûres des TIC;

14) assistance à la sensibilisation et identification d'aspects fondamentaux pour favoriser une culture de la cybersécurité; recommandation de bonnes pratiques-types pour renforcer les applications des TIC et limiter les cybermenaces;

15) élaboration d'instruments pour faciliter l'échange d'informations sur des aspects technologiques et politiques et sur les bonnes pratiques en matière de cybersécurité.

5.3 Investissement accru dans la sensibilisation et l'éducation du public

1) Elaboration de stratégies mondiales visant à faciliter le renforcement des capacités humaines et institutionnelles.

2) Formation destinée aux professionnels de la justice pénale.

3) Incitation du secteur privé à rapporter toute information pouvant lui parvenir concernant la cybercriminalité aux autorités compétentes des services sociaux ou des organes responsables de l'application des lois.

5.4 Protection en ligne des enfants

Par ailleurs, la nature même d'Internet abolit les frontières, caractéristique qu'une sécurité en ligne efficace doit reconnaître pour exploiter ce qu'il y a de mieux dans le monde. Des stratégies efficaces de protection en ligne doivent tirer des enseignements des réussites et des erreurs des autres, notamment des pays arabes voisins, et rester attentives au développement mondial et aux tendances émergentes. Les recommandations ci-dessous respectent ces principes et sont à prendre en compte dans le cadre national de la protection en ligne des enfants dans les pays arabes; elles ont été abordées et adoptées lors de l'atelier régional de l'UIT sur la défense de la politique à mener et le renforcement des capacités en matière de protection en ligne des enfants dans le monde arabe, réuni à Mascate, dans le sultanat d'Oman, les 30 et 31 octobre.

1) Encourager tous les pays arabes à appuyer l'initiative de protection en ligne des enfants (COP) de l'UIT.

2) Unifier et coordonner tous les efforts de sensibilisation pour l'initiative pour la Protection en ligne des enfants (COP) dans la région.

3) Créer un "portail des enfants du monde arabe", financé par l'UIT et la Ligue des Etats arabes, et le mettre en ligne sur le site web de l'Observatoire panarabe pour la sûreté et la cybersécurité.

4) Encourager les pays arabes à élaborer des politiques et des stratégies qui protègeraient les enfants dans le cyberespace et promouvraient la sécurité de leur accès.

5) Echanger des bonnes pratiques, en particulier l'expérience de Bahreïn, et signer un protocole d'accord avec l'Autorité régulatrice des télécommunications de Bahreïn pour faire bénéficier les autres pays de cette expérience.

6) Promouvoir la coopération régionale et internationale et unir les efforts pour échanger des conseils et des informations.

7) Encourager les Etats arabes à adopter des procédures juridiques favorisant la promotion et le soutien des fabricants locaux dans le cadre de la création de logiciels spécifiques et de contenus en arabe pour l'initiative de Protection en ligne des enfants.

8) Instaurer des mécanismes de promotion du partenariat entre les gouvernements et les fabricants de logiciels, afin d'apporter les solutions les plus sûres à l'initiative de Protection en ligne des enfants.

9) Trouver la manière d'obliger les cybercafés de tous les Etats arabes à utiliser les navigateurs Internet pour mineurs pour la Protection en ligne des enfants.

ANNEXE

Objectifs et moyens du Sommet
(tels qu'ils ont été identifiés par le groupe de travail sur la confiance et la sécurité)

Objectifs

1) Mettre en place un accord panarabe sur la cybersécurité et la cybercriminalité, qui soit conforme aux normes et aux principes internationaux existants et qui renforce la coopération mondiale dans ces domaines.

2) Elaborer des stratégies nationales relatives à la cybersécurité, alignées sur les principes de coopération internationaux, y compris la Protection des infrastructures essentielles de l'information (CIIP), dans un délai de 5 ans.

3) Etablir, dans tous les pays arabes, des cadres juridiques nationaux harmonisés à l'échelle régionale, dans un délai de 5 ans.

4) Etablir un programme d'études relatives à la cybersécurité visant à renforcer les capacités et à sensibiliser diverses parties prenantes (par exemple, les gouvernements, les milieux universitaires, le secteur privé et les écoles).

5) Créer des Equipes d'intervention en cas d'incident lié à la sécurité informatique (CSIRT/des équipes d'intervention en cas d'urgence informatique (CERT) dans les pays arabes où de telles équipes n'existent pas, dans un délai de trois ans.

6) Souligner l'importance de l'initiative pour la Protection en ligne des enfants (COP) et de la sécurité des enfants et des jeunes, au moyen de programmes de sensibilisation et de mesures techniques.

Moyens

1) Jouer un rôle actif lors des débats et des activités liés aux politiques publiques internationales relatives à Internet.

2) Instaurer un groupe de travail composé d'experts, au mandat et aux responsabilités clairs, ayant pour but:

   a) d'entreprendre une analyse détaillée dans la région (sous forme d'une étude) afin d'identifier ses lacunes et d'élaborer une feuille de route pour mettre en oeuvre les objectifs définis et des mesures visant à combler ces lacunes;

   b) de mettre en route le processus de transfert de savoir-faire et d'échange d'informations entre les pays arabes, en ayant recours aux bonnes pratiques régionales et nationales ainsi qu'aux exemples de réussites, afin de mieux aider les pays en ayant besoin.

3) Encourager les investissements et les partenariats public-privé.

_____