Forum régional UIT 2009 sur la cybersécurité pour l'Afrique et les Etats arabes

"Connecter le monde de façon responsable"

Tunis, Tunisie
4 et 5 juin 2009

Ordre du jour du Forum

Description: Les technologies de l'information et de la communication (TIC) jouent un rôle décisif dans le développement d'un pays. Pourtant, parallèlement, la croissance rapide des réseaux TIC ouvre aux criminels de nouvelles voies pour exploiter les points faibles de la Toile et s'en prendre aux infrastructures essentielles des pays. Rendre l'utilisation des TIC plus sûre est donc l'un des défis les plus importants et les plus complexes que doivent aujourd'hui relever les pays. Les notions de frontières nationales étant, dans une grande mesure, absentes du cyberespace et les cybermenaces pouvant surgir partout et à tout moment et causer de très graves dégâts en un bref laps de temps avant qu'on puisse y remédier, les tentatives actuelles visant à résoudre ces problèmes sur les seuls plans national et régional sont insuffisantes. Il faut impérativement envisager la situation dans une optique mondiale. C'est pourquoi l'UIT, avec son Programme mondial cybersécurité (GCA), a mis en place un cadre de coopération internationale dans ce domaine.

La cybersécurité et la protection des infrastructures essentielles de l'information relèvent de la responsabilité des pouvoirs publics, mais aussi du secteur privé, des organisations, et des particuliers qui les utilisent – autrement dit, de tous ceux qui mettent au point, possèdent, fournissent, gèrent, entretiennent et utilisent les technologies, systèmes et réseaux de l'information et de la communication. La promotion de la cybersécurité et la mise en œuvre des mesures correspondantes doivent figurer parmi les premières priorités des pays pour qu'ils puissent exploiter pleinement les avantages de la révolution du numérique et des nouvelles technologies de la communication, en pleine évolution.

Le Forum régional UIT 2009 sur la cybersécurité pour l'Afrique et les Etats arabes, dont le thème est **"Connecter le monde de façon responsable"**, a pour objet de définir certains des principaux problèmes auxquels font face les pays de la région lorsqu'il s'agit de renforcer la cybersécurité et de sécuriser les infrastructures essentielles de l'information. Les participants à ce Forum analyseront des bonnes pratiques, des mécanismes d'échange d'informations et des mesures concrètes de renforcement de la cybersécurité, compte tenu de principes fondamentaux tels que la prise en compte de l'absence de frontières dans le cyberespace et du caractère transnational des cybermenaces, tout en répondant à des besoins précis aux niveaux national et régional. Ils examineront en outre les mesures que les pays de la région ont prises ou prévoient de prendre pour renforcer la coopération et la collaboration avec d'autres parties prenantes sur les plans national, régional et international.

JEUDI 4 JUIN 2009	
08:30–09:30	**Inscription à la réunion et retrait des badges (Inscription préalable en ligne obligatoire)**
09:30–10:00	**Ouverture de la réunion et allocution de bienvenue**
	Allocution de bienvenue *Remarques liminaires* *Remarques liminaires*

10:00–11:15	**Session 1: Le contexte — Vers une approche intégrée de la cybersécurité et de la protection des infrastructures essentielles de l'information (CIIP)**
	Description: La confiance et la sécurité dans l'utilisation des TIC sont essentielles à l'édification d'une société de l'information inclusive, sûre et universelle. L'évolution permanente de l'utilisation des TIC, des systèmes et des réseaux présente certes des avantages incontestables. Toutefois, face à cette évolution, les pouvoirs publics, mais aussi le secteur privé, les organisations, et les particuliers qui utilisent ces technologies – autrement dit, tous ceux qui mettent au point, possèdent, fournissent, gèrent, entretiennent et utilisent ces réseaux – doivent faire davantage porter leurs efforts sur la cybersécurité et la protection des infrastructures essentielles de l'information. En raison des interconnexions entre les TIC, on ne peut véritablement promouvoir la cybersécurité que si toutes les parties prenantes sont conscientes des dangers et des menaces existants et savent comment se protéger dans leurs activités en ligne. Les pouvoirs publics ont un rôle de premier plan à jouer pour promouvoir une culture de la cybersécurité et soutenir les efforts d'autres parties prenantes à cet égard. En outre, la coopération régionale et internationale est essentielle pour encourager une culture mondiale de la cybersécurité. Les participants à cette session examineront les cybermenaces dans le contexte actuel et cerneront les défis que doivent relever les pays, les entreprises et les particuliers pour gérer le quotidien dans un environnement qui ne cesse d'évoluer.
11:15–11:30	**Pause-café**
11:30–13:00	**Session 2: Concilier les enjeux mondiaux et les besoins nationaux et régionaux**
	Description: L'UIT, avec son Programme mondial cybersécurité (GCA), a mis en place un cadre international de coopération en matière de cybersécurité – tribune mondiale dans le cadre de laquelle toutes les parties prenantes intéressées peuvent débattre et collaborer afin de résoudre au mieux et de manière coordonnée les problèmes de cybersécurité, de plus en plus préoccupants. Toutefois, chaque pays et chaque région ont leurs propres impératifs et besoins, dont il faut tenir compte dans le contexte national et régional. L'UIT, avec la coopération de ses Etats Membres, s'efforce de tenir compte de ces besoins pour que l'aide apportée soit efficace. Les participants à cette session se demanderont comment une approche ascendante ou descendante peut contribuer à harmoniser les efforts globaux en vue de fournir aux Etats Membres une réponse et une assistance intégrées et cohérentes.
13:00–14:30	**Déjeuner**
14:30–15.45	**Session 3: La cybersécurité dans les programmes nationaux et les mesures à envisager lors de l'élaboration d'une stratégie nationale en matière de cybersécurité**
	Description: La nécessité de renforcer la confiance et la sécurité dans l'utilisation des TIC, de promouvoir la cybersécurité et de protéger les infrastructures essentielles sur le plan national est généralement reconnue. Alors que les professionnels des secteurs public et privé ont leur propre conception de ces questions importantes, dans un souci de cohérence, certains pays ont, dans le domaine de la cybersécurité/CIIP, mis en place des cadres institutionnels, tandis que d'autres préfèrent une approche plus souple et moins formelle. Quels sont les problèmes à prendre en compte dans l'élaboration d'une stratégie nationale de cybersécurité et de protection des infrastructures essentielles de l'information? Quels professionnels doivent prendre part à cette réflexion? Les participants à cette session débattront de certains des éléments nécessaires à l'élaboration et à l'organisation des efforts déployés par les pays en matière de cybersécurité/CIIP. Ils se familiariseront aussi avec le kit pratique mis au point par l'UIT pour l'auto-évaluation nationale en matière de cybersécurité/CIIP, destiné à aider les pouvoirs publics des différents pays à examiner leurs politiques, procédures, normes, institutions et relations existantes, à la lumière des besoins nationaux pour renforcer la cybersécurité et protéger les infrastructures essentielles de l'information.

15:45–16:00	**Pause-café/thé**
16:00–17:15	**Session 4: Mesures concrètes visant à promouvoir la coopération aux niveaux régional et international**
	Description: La coopération régionale et internationale est fondamentale pour encourager les efforts en matière de cybersécurité et faciliter le dialogue et les échanges. Les problèmes posés par les cyberattaques et la cybercriminalité, qui ont une envergure universelle et sont lourds de conséquences, ne peuvent être traités que dans le cadre d'une stratégie cohérente placée sous le signe de la coopération internationale, compte tenu des rôles des différentes parties prenantes et des initiatives existantes. En tant que coordonnatrice de la grande orientation C5 du SMSI, dont le thème est "Etablir la confiance et la sécurité dans l'utilisation des TIC", l'UIT procède à des échanges de vues avec les principales parties prenantes quant à la meilleure façon de riposter de manière concertée aux menaces de plus en plus préoccupantes pour la cybersécurité. Les participants à cette session passeront en revue certaines des initiatives régionales en cours pour alimenter les débats, afin de déterminer de possibles mesures et actions concrètes à prendre pour promouvoir la coopération régionale et internationale en vue de renforcer la cybersécurité.
17:15–17:30	**Synthèse de la journée et annonces**
19:00–	**Réception**

VENDREDI 5 JUIN 2009	
09:30 –10:45	**Session 5: Etablir des bases juridiques et mettre en place des moyens d'application efficaces**
	Description: Pour prévenir, détecter et réprimer la cybercriminalité et l'utilisation délictueuse des TIC, il faut une législation nationale adaptée, ainsi qu'une coordination juridique et des mesures exécutoires sur le plan international. A cette fin, il est nécessaire d'actualiser les dispositions, les procédures et les grands principes du droit pénal afin qu'ils prennent en compte les incidents en matière de cybersécurité et luttent contre la cybercriminalité. De nombreux pays ont par conséquent modifié leur code pénal ou ont entrepris de le faire, conformément aux cadres et recommandations existant sur le plan international. Les participants à cette session réfléchiront à la nécessité d'établir de bonnes bases juridiques et d'adopter des mesures exécutoires efficaces, examineront certaines méthodes juridiques adoptées sur le plan national et se demanderont dans quels domaines la coordination juridique pourrait être intensifiée entre les pays.
10:45–11:00	**Pause-café/thé**
11:00–12:45	**Session 6: Réfléchir aux solutions techniques relatives à la résilience des réseaux d'information et de communication**
	Description: L'expansion et l'évolution des télécommunications ouvrent de nouvelles perspectives, mais parallèlement sont source de nouveaux problèmes. La convergence et le passage aux réseaux fondés sur le protocole Internet (IP) ou aux réseaux de prochaine génération (NGN) imposent de redéfinir les stratégies sectorielles et commerciales. De nouveaux services et de nouvelles applications, comme le protocole voix sur Internet (VoIP), remettent en question les modèles économiques et les cadres réglementaires. Face à cette transition, les pouvoirs publics, les régulateurs, les opérateurs et les équipementiers s'efforcent d'anticiper et de s'adapter aux enjeux de demain. Les participants à cette session examineront les menaces auxquelles doivent faire face les réseaux ainsi que les mesures et les normes techniques pouvant être adoptées pour améliorer la résilience de ces réseaux. Cette session a pour objectif d'aider les pays à mieux comprendre comment atténuer l'impact des menaces sur la sécurité et de faire en sorte que les communications utilisant les réseaux publics de télécommunication restent fiables, sûrs, interopérables et faciles à utiliser.
12:45–14:00	**Déjeuner**
14:00–15:30	**Session 7: Définir des structures administratives solides et mettre en place des capacités de gestion des incidents**
	Description: La solution aux problèmes de cybersécurité passe par la mise en place de capacités de veille, d'alerte et de réaction en cas de cyberincident afin de prévoir, de détecter, de gérer ce type d'incident et d'y remédier. Une gestion efficace de ces incidents nécessite une réflexion sur de multiples éléments: financement, ressources humaines, formation, capacités technologiques,

	collaboration entre secteur public et secteur privé et impératifs juridiques. Une collaboration à tous les niveaux de l'Etat ainsi qu'avec le secteur privé, les universitaires et les organisations régionales et internationales est nécessaire pour sensibiliser le public aux attaques potentielles et aux mesures à prendre pour y remédier. Les participants à cette session discuteront des bonnes pratiques, des structures administratives et des normes connexes en ce qui concerne les aspects techniques, administratifs et financiers de la création d'équipes nationales, régionales et internationales ayant des responsabilités en matière de veille, d'alerte et d'intervention en cas d'incident.
15:30–15:45	**Pause-café/thé**
15:45–17:00	**Session 8: Promouvoir une culture de la cybersécurité dans le cadre de partenariats novateurs**
	Description: Au vu de la réalité du cyberespace, il est évident que nous devons tous collaborer. Pour trouver une parade efficace aux cybermenaces, il faut pouvoir disposer de ressources, de compétences techniques et d'investissements solides visant à développer les capacités - tous efforts qui ne peuvent être entrepris par une entité à elle seule. L'élément clé est de réunir les secteurs public et privé dans le cadre de forums et d'activités communes afin de faire face aux problèmes de cybersécurité et de mettre au point de solides programmes de renforcement des capacités. Tous les internautes devraient participer à ces efforts, qu'il s'agisse de particuliers ou d'entreprises, de représentants de l'ordre ou encore de fournisseurs d'infrastructures essentielles. La clé de la réussite d'un partenariat est la confiance, qui est nécessaire pour établir, développer et entretenir des relations de partage entre les différentes parties. Les participants à cette session s'intéresseront de près aux avantages et aux problèmes liés à la création de partenariats durables et innovants visant à améliorer la cybersécurité et se demanderont comment les efforts conjoints permettent de progresser concrètement.
17:00 –17:30	**Session 9: Synthèse du Forum, recommandations et solutions**
	Description: Les participants à la session finale rendront compte des principales conclusions du Forum et s'efforceront de définir des recommandations pour l'avenir afin d'améliorer la cybersécurité et la protection des infrastructures essentielles de l'information dans la région.
17:30 –18:00	**Clôture de la réunion**
	Remarques de clôture *Remarques liminaires*