

RÉSOLUTION 69 (Rév. Bakou, 2025)

**Faciliter la création et le renforcement d'équipes nationales
d'intervention en cas d'incident informatique, en particulier
pour les pays en développement, et la
coopération entre ces équipes**

La Conférence mondiale de développement des télécommunications (Bakou, 2025),

rappelant

- a)* les Résolutions 101 (Rév. Bucarest, 2022), 102 (Rév. Bucarest, 2022) et 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires, qui soulignent la nécessité d'une collaboration;
- b)* la Résolution 58 (Rév. New Delhi, 2024) de l'Assemblée mondiale de normalisation des télécommunications (AMNT), intitulée "Encourager la création et le renforcement d'équipes nationales d'intervention en cas d'incident informatique, en particulier pour les pays en développement"¹;
- c)* la Résolution 50 (Rév. New Delhi, 2024) de l'AMNT relative à la cybersécurité;
- d)* la Résolution 214 (Bucarest, 2022) de la Conférence de plénipotentiaires, relative aux technologies d'intelligence artificielle (IA) et aux télécommunications/technologies de l'information et de la communication (TIC), qui définit le cadre dans lequel le Directeur du Bureau de développement des télécommunications (BDT) peut appuyer les travaux du Secteur du développement des télécommunications de l'UIT (UIT-D) visant à relever les défis posés et à tirer parti des possibilités offertes par l'IA en tant que technologie nouvelle et émergente, lorsqu'elle est appliquée aux équipes nationales d'intervention en cas d'incident informatique (CIRT) dans le traitement des incidents de cybersécurité,

reconnaissant

- a)* que les pays en développement utilisent de plus en plus l'ordinateur et en sont de plus en plus tributaires pour les TIC;

¹ Par pays en développement, on entend aussi les pays les moins avancés, les petits États insulaires en développement, les pays en développement sans littoral et les pays dont l'économie est en transition.

- b)* que les pays en développement sont exposés à des menaces de cybersécurité et des attaques visant les réseaux des TIC et qu'ils pourraient être mieux préparés à faire face à de tels incidents de cybersécurité et aux activités frauduleuses de plus en plus nombreuses menées par ce biais;
- c)* qu'il est nécessaire d'améliorer la coopération et la capacité à faire face aux problèmes de cybersécurité;
- d)* les résultats des travaux menés à ce jour par la Commission d'études 2 de l'UIT-D au titre de la Question 3/2 et les rapports que cette Commission a établis sur ce sujet, dans lesquels elle appuie notamment la création et la coordination d'équipes CIRT et la conclusion de partenariats entre secteur public et secteur privé;
- e)* les travaux menés à ce jour par le BDT afin que les États Membres et d'autres parties prenantes s'associent pour aider les pays à se doter de capacités de gestion des incidents au niveau national, par exemple d'équipes CIRT;
- f)* qu'il est important d'avoir un niveau approprié de préparation aux situations d'urgence de cybersécurité dans tous les pays, en particulier dans les pays en développement, en créant des équipes CIRT au niveau national, et qu'il est important d'assurer une coordination à l'intérieur des régions et entre les régions et de tirer parti des initiatives régionales ou internationales prises à cet égard, notamment de la coopération entre l'UIT et des projets régionaux ou mondiaux ainsi que des organisations régionales ou mondiales, comme le Forum des équipes de sécurité et d'intervention en cas d'incidents (FIRST), l'Organisation des États américains et l'Équipe CIRT pour la région Asie-Pacifique, notamment;
- g)* que les télécommunications/TIC émergentes sont actuellement utilisées dans le cadre des mesures techniques de lutte contre les attaques et menaces de cybersécurité;
- h)* les travaux pertinents de la Commission d'études 17 du Secteur de la normalisation des télécommunications de l'UIT (UIT-T), notamment sur les techniques d'échange d'informations sur la cybersécurité;
- i)* que les pays pourraient bénéficier d'une coordination entre équipes CIRT sectorielles nationales, lorsque celles-ci existent, afin d'améliorer la gestion des incidents en cas d'incident majeur de cybersécurité ayant des répercussions touchant plusieurs secteurs au niveau national;
- j)* les résultats des efforts fournis par l'UIT-T concernant l'évaluation, la conception, la création, le renforcement et la collaboration des équipes CIRCT nationales,

notant

- a) que le niveau de préparation aux situations d'urgence en matière de cybersécurité s'améliore, mais reste faible dans les pays en développement;
- b) que le degré d'interconnectivité élevé des réseaux de télécommunication/TIC pourrait être affecté en cas d'attaques et menaces de cybersécurité provenant de réseaux de pays moins bien préparés, qui, pour l'essentiel, sont des pays en développement;
- c) que les pays pourraient faire face à de nouvelles difficultés importantes et bénéficier de nouvelles possibilités dans le traitement des incidents de cybersécurité, à mesure que des services et technologies de télécommunication/TIC nouveaux et émergents continuent de se développer;
- d) le point *i)* du *considérant* de la Résolution 130 (Rév. Bucarest, 2022) de la Conférence de plénipotentiaires, qui dispose que, pour protéger ces infrastructures et traiter ces problèmes et ces menaces, il faut que des mesures coordonnées soient prises aux niveaux national, régional et international en matière de prévention, de préparation, de réaction et de rétablissement en cas d'incidents liés à la sécurité informatique, par les autorités nationales (y compris la création d'équipes CIRT) et sous nationales, par le secteur privé, et par les particuliers et les utilisateurs; une coopération et une coordination internationales et régionales sont également nécessaires et l'UIT a un rôle prééminent à jouer dans le cadre de son mandat et de ses compétences en la matière;
- e) que, pour être efficace et viable, la création d'équipes CIRT et leur renforcement nécessitent l'affectation en permanence de ressources appropriées;
- f) les travaux de la Commission d'études 17 de l'UIT-T dans le domaine des équipes nationales CIRT, en particulier pour les pays en développement, et la coopération entre ces équipes, comme indiqué dans les documents établis par cette commission d'études;
- g) qu'il est nécessaire de créer des équipes CIRT au niveau national, selon qu'il convient, y compris des équipes CIRT chargées de la coopération entre les gouvernements, et qu'il est important d'assurer une coordination entre toutes les organisations concernées;
- h) le Programme mondial cybersécurité (GCA) de l'UIT et les lignes directrices relatives à l'utilisation de ce programme par l'UIT, approuvées par le Conseil;

i) l'utilisation croissante des télécommunications/TIC nouvelles et émergentes dans tous les aspects du quotidien, y compris le passage au tout numérique pour les services publics, qui nécessitent un niveau de protection élevé;

j) que les équipes CIRT peuvent contribuer à répondre à la nécessité impérieuse de renforcer la sécurité et la confiance dans l'utilisation des TIC,

décide

1 de faciliter la création et le renforcement des équipes CIRT nationales dans les États Membres lorsqu'un appui a été demandé, selon les besoins, dans les limites des ressources budgétaires existantes;

2 d'encourager l'UIT-D à poursuivre ses travaux concernant l'évaluation, la conception, la création, le renforcement et la collaboration des équipes CIRT nationales,

charge le Directeur du Bureau de développement des télécommunications

1 d'encourager, aux niveaux national, régional et international, l'adoption de bonnes pratiques relatives à l'établissement et au renforcement d'équipes CIRT et de centres d'échange et d'analyse des informations, telles que définies à ce jour par les commissions d'études compétentes de l'UIT, par exemple, dans le cadre de l'ancienne Question 3/2 confiée à la Commission d'études 2 de l'UIT-D et la Commission d'études 17 de l'UIT-T, et par d'autres organisations et experts concernés;

2 de renforcer les capacités des équipes CIRT nationales, en particulier dans les domaines des technologies et des services de télécommunication/TIC nouveaux et émergents, par l'intermédiaire des bureaux régionaux et des bureaux de zone de l'UIT, notamment sous la forme d'un appui pour l'évaluation continue de la maturité, compte tenu des ressources financières;

3 d'apporter un appui aux équipes CIRT nationales, en particulier dans les pays en développement, en échangeant des orientations et des bonnes pratiques concernant les problèmes et les possibilités liés aux services et aux technologies de télécommunication/TIC nouveaux et émergents dans le cadre des interventions en cas d'incident de cybersécurité;

4 d'apporter un appui aux équipes CIRT nationales à améliorer les échanges d'information et la collaboration et à diffuser des bonnes pratiques aux fins des interventions en cas d'incident de cybersécurité, afin d'accroître le niveau de préparation aux situations d'urgence y afférentes, en particulier dans les pays en développement, partout dans le monde;

5 de promouvoir les cadres opérationnels connexes applicables aux équipes CIRT dans les États Membres où de telles équipes sont constituées, le cas échéant;

6 de continuer de mobiliser des ressources afin de promouvoir les programmes de formation nécessaires dans ce domaine, y compris des parcours d'apprentissage à plusieurs niveaux (élémentaire, intermédiaire et avancé) pour favoriser un renforcement progressif des capacités, et en continuant d'apporter l'appui approprié aux pays en développement qui le souhaitent;

7 de promouvoir les bonnes pratiques relatives à l'établissement d'une structure nationale chargée de coordonner les équipes CIRT sectorielles nationales, lorsque de telles équipes existent, et d'améliorer la gestion des incidents en cas d'incidents de cybersécurité majeurs touchant plusieurs secteurs au niveau national;

8 de continuer de favoriser la collaboration entre les équipes CIRT nationales et au sein de ces équipes, y compris les équipes CIRT chargées de la coopération entre les gouvernements, les équipes CIRT du secteur privé, et les équipes CIRT d'établissements universitaires, conformément à la législation nationale, aux niveaux régional et mondial, en encourageant la participation des pays en développement à des projets régionaux ou mondiaux et aux travaux des organisations concernées, comme le Forum FIRST, et des organisations régionales, notamment;

9 d'œuvrer à la réalisation de ces objectifs tout en évitant la répétition des tâches avec d'autres organisations;

10 de continuer à élaborer des programmes pour des campagnes de sensibilisation sur l'importance de créer des équipes CIRT et de les renforcer pour accroître le niveau du dispositif de cybersécurité;

11 de continuer d'améliorer les kits pratiques existants que les pays en développement pourraient utiliser pour organiser des exercices de simulation ou des entraînements d'intervention en cas d'incident,

invite les États Membres

1 à créer des équipes CIRT nationales, y compris des équipes CIRT chargées de la coopération entre les gouvernements, lorsque de telles équipes sont nécessaires ou font actuellement défaut, selon qu'il conviendra;

2 à améliorer la maturité, les capacités et la résilience des équipes CIRT mises en place, pour faire face efficacement à l'évolution des menaces de cybersécurité;

3 à contribuer à l'élaboration d'une plate-forme de ressources d'information, conformément à la Décision 630 (C23) du Conseil, contenant un répertoire tenu à jour des bonnes pratiques en matière de création et de gestion d'équipes CIRT nationales;

4 à collaborer étroitement avec l'UIT-D, l'UIT-T et d'autres organisations compétentes, en tenant compte de la Résolution 58 (Rév. New Delhi, 2024) de l'AMNT, selon qu'il conviendra;

5 à promouvoir et à faciliter l'échange de bonnes pratiques entre leurs équipes CIRT nationales, y compris en participant aux initiatives pertinentes de ces équipes, dont le Forum FIRST;

6 à encourager l'utilisation des télécommunications/TIC nouvelles et émergentes pour améliorer les capacités techniques des équipes CIRT;

7 à envisager, s'il y a lieu, de créer une structure nationale de coordination entre les équipes CIRT nationales sectorielles, si elles existent, afin d'améliorer la gestion lors d'incidents majeurs de cybersécurité et de produire des effets dans plusieurs secteurs;

8 à encourager le partage volontaire d'informations sur les menaces et les vulnérabilités en matière de cybersécurité entre les États Membres, y compris par le biais des plates-formes d'échange d'informations existantes;

9 à faire part de leurs besoins aux bureaux régionaux et aux bureaux de zone de l'UIT,

invite les Membres de Secteur, les Associés et les établissements universitaires, selon qu'il conviendra

1 à œuvrer à la création et au renforcement d'équipes CIRT nationales, en particulier pour les pays en développement;

2 à apporter un appui suffisant aux activités de renforcement des compétences relatives aux services et aux technologies de télécommunication/TIC nouveaux et émergents par les équipes CIRT nationales, en particulier pour les pays en développement;

3 à contribuer aux débats, aux échanges d'informations, au renforcement des capacités et aux études sur les difficultés auxquelles sont confrontées les équipes CIRT nationales et les possibilités qui s'offrent à elles s'agissant de répondre aux incidents de cybersécurité, étant donné que les technologies fondées sur l'intelligence artificielle continuent d'évoluer et d'être utilisées dans le domaine des télécommunications/TIC, de façon à rendre ces dernières plus efficaces et plus performantes.