27 juillet 2020
Français
Original : anglais

Groupe d'experts chargé de réaliser une étude approfondie sur la cybercriminalité
Vienne, 27-29 juillet 2020

Projet de rapport

Additif

II. Liste de recommandations et conclusions préliminaires (*suite*)

B. Prévention

1. Conformément au plan de travail du Groupe d'experts, le présent paragraphe contient une compilation de propositions formulées à la réunion par les États Membres au titre du point 3 de l'ordre du jour, intitulé « Prévention ». Ces recommandations et conclusions préliminaires ont été faites par les États Membres et leur inclusion ne signifie pas qu'elles ont l'aval du Groupe d'experts et leur ordre de présentation ne reflète pas leur degré d'importance :

1) Il convient de reconnaître que la prévention n'est pas seulement la responsabilité des États, mais qu'elle exige la participation de toutes les parties prenantes, y compris des services répressifs, du secteur privé, en particulier des fournisseurs d'accès à Internet, des organisations non gouvernementales, des écoles et des universités ainsi que du public en général ;

2) Il a été recommandé que le public puisse aisément accéder aux outils de prévention tels que les plateformes en ligne, les clips audio, les infographies dans un langage simple, ainsi qu'aux plateformes de signalement ;

3) Il a été jugé nécessaire d'élaborer un ensemble de politiques publiques de prévention à long terme, qui devraient inclure l'élaboration de campagnes de sensibilisation sur l'utilisation sûre d'Internet ;

4) Les activités de sensibilisation à la cybersécurité devraient figurer dans le programme de l'enseignement primaire, secondaire et supérieur, tant pour les étudiants que pour les enseignants. Idéalement, elles devraient faire partie intégrante des stratégies nationales en matière de cybersécurité. Par ailleurs, les États devraient mettre en commun leurs expériences sur la manière d'utiliser ces stratégies de cybersécurité pour prévenir la cybercriminalité. Ils devraient en outre accorder une attention particulière aux mesures préventives destinées aux jeunes, y compris aux primo-délinquants, afin de prévenir la récidive ;

5) Dans le cadre de la prévention et de la lutte contre la cybercriminalité, les États devraient accorder une attention particulière aux questions de prévention et

d'éradication de la violence sexiste, de la violence à l'égard des femmes et des filles et des crimes de haine ;

6) Les activités de prévention doivent être proactives, régulières et continues et adaptées aux groupes vulnérables ;

7) Les interactions et la collaboration entre les secteurs public et privé, compte tenu des jeux de données volumineuses ou des centres de données volumineuses, peuvent présenter une forte vulnérabilité, en particulier (mais pas seulement) dans le secteur de la santé, compte tenu de la pandémie actuelle. Les États devraient accorder une attention particulière à la réglementation de l'accès légal à ces données et à leur protection contre les attaques des cyberdélinquants ;

8) En ce qui concerne les efforts de prévention, les FAI devraient assumer une plus grande responsabilité en matière de mesures de sécurité (« par défaut ») et de prévention de la cybercriminalité, et des normes internationales devraient être élaborées sur le contenu et la durée des informations de journal à conserver par les FAI. En outre, les responsabilités des FAI en matière de détection, de prévention et de répression de la cybercriminalité devraient être clairement définies ;

9) Des partenariats public-privé sont nécessaires pour prévenir et combattre la cybercriminalité, y compris la coopération avec les acteurs de la cybersécurité et les grandes entreprises technologiques en matière de partage d'informations ;

10) Les États devraient dispenser une formation aux magistrats et juges spécialisés qui traitent des affaires de cybercriminalité et fournir aux organismes d'enquête des outils performants pour tracer les cryptomonnaies et lutter contre leur utilisation à des fins criminelles ;

11) Les États devraient renforcer les stratégies visant à lutter contre l'utilisation, par les groupes criminels traditionnels, d'outils électroniques pour dissimuler leurs communications et leurs activités ;

12) Des solutions devraient être élaborées aux fins d'une coopération directe entre les autorités nationales et les fournisseurs d'accès à Internet, tout en respectant l'état de droit et les droits humains, y compris les exigences en matière de protection des données ;

13) Les États devraient garantir la liberté de la presse lorsqu'ils élaborent des mesures de prévention de la cybercriminalité ;

14) Il a été recommandé de renforcer les capacités collectives des institutions compétentes et, en termes de prévention, de passer d'une culture réactive à une culture proactive. Il a également été recommandé de mettre en place un mécanisme solide pour stimuler et faciliter le partage de renseignements sur les modes opératoires possibles des délinquants ;

15) Les États Membres sont encouragés à continuer d'adopter des mesures de prévention efficaces aux niveaux national et international et à se concentrer sur des activités en amont telles que la sensibilisation aux risques de cybercriminalité ; les campagnes axées sur des modes opératoires tels que le phishing ou les logiciels malveillants (« ransomware ») et sur différents groupes tels que les jeunes ou les personnes âgées ; la probabilité de poursuivre et de punir les délinquants et les efforts de prévention de la criminalité par l'identification et la répression des activités illicites en ligne. Les services de police et le ministère public doivent investir dans des stratégies visant à détecter, signaler et intervenir face aux menaces que représente la cybercriminalité. Il est important de noter qu'ici aussi, les partenariats public-privé sont indispensables. Ces activités de prévention ne requièrent pas de lois ou de règlements supplémentaires ;

16) En raison de l'existence d'une « fracture numérique », certains pays en développement n'ont pas les moyens de prévenir, de détecter et de combattre la cybercriminalité, et sont plus vulnérables face aux défis que pose la cybercriminalité ;

17) L'ONUDC a été vivement encouragé à continuer à fournir une assistance technique aux États qui en font la demande, pour prévenir et combattre la cybercriminalité.