

CyberSud+ projet visant le renforcement de la coopération en matière de cybercriminalité et de preuves électroniques dans la région du Voisinage Sud

Titre du projet :	CyberSud+ : Coopération renforcée en matière de cybercriminalité et de preuves électroniques dans la région du Voisinage Sud
Zone du projet :	Pays prioritaires : Algérie, Egypte, Jordanie, Liban, Libye, Maroc, Palestine* et Tunisie
Durée proposée :	36 mois (1 janvier 2024 – 31 décembre 2026)
Budget proposé :	3,89 millions EUR
Financement :	Union européenne (90%) et Conseil de l'Europe (10%)
Mise en œuvre :	Bureau des Programmes sur la cybercriminalité du Conseil de l'Europe (C-PROC)

Contexte et justification

Les pays de la région du sud de la Méditerranée – à l'instar des sociétés du monde entier – s'appuient de plus en plus sur les technologies de l'information et de la communication (TIC), mais cela les rend également vulnérables à des menaces telles que la cybercriminalité. La cybercriminalité – c'est-à-dire les infractions commises contre des systèmes informatiques et au moyen d'ordinateurs – touche les particuliers, les institutions et les organisations, ainsi que les États. La multiplication des attaques par ransomware et d'autres types d'attaques contre les infrastructures d'information critiques souligne la nécessité de créer des synergies entre les réponses pénales à la cybercriminalité et les mesures visant à renforcer la cybersécurité.

De plus, les preuves relatives à tout crime sont désormais souvent stockées sur des systèmes informatiques. Il est nécessaire de mettre en place une réponse pénale aux défis posés par la cybercriminalité et les preuves électroniques qui soit à la fois efficace et conforme aux exigences en matière de droits de l'homme et d'État de droit. [La Convention sur la cybercriminalité \(Convention de Budapest\) et ses protocoles](#) offrent un cadre pour une telle réponse pénale. Le Maroc et la Tunisie sont parties à la Convention, tandis que plusieurs autres pays de la région ont adapté ou sont en train d'adapter leur droit pénal national aux exigences de la Convention.

Le nouveau [Deuxième Protocole additionnel à ce traité sur le renforcement de la coopération et la divulgation des preuves électroniques](#) qui a été ouvert à la signature en mai 2022 fournit de nouveaux outils innovants.¹ Le Maroc a été parmi les signataires en mai 2022.

* Cette désignation ne doit pas être interprétée comme une reconnaissance de l'État de Palestine et ne préjuge en rien des positions individuelles des États membres du Conseil de l'Europe et de l'Union européenne sur cette question.

¹ Les outils de ce Protocole comprennent : la coopération directe avec les fournisseurs de services des autres Parties pour la divulgation d'informations relatives aux abonnés et avec les bureaux d'enregistrement pour les informations relatives à l'enregistrement des noms de domaine ; la coopération de gouvernement à gouvernement pour la production d'informations relatives aux abonnés et de données

Le Conseil de l'Europe et l'Union européenne travaillent avec l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie depuis 2017 à travers le projet conjoint [CyberSud](#) visant à renforcer « la législation et les capacités institutionnelles en matière de cybercriminalité et de preuves électroniques dans la région du Voisinage Sud, conformément aux exigences en matière de droits de l'homme et d'État de droit ».

CyberSud+ vise à renforcer les capacités en matière de justice pénale afin d'améliorer la coopération dans le domaine de la cybercriminalité et la communication des preuves électroniques, grâce à une combinaison d'actions régionales et spécifiques à chaque pays, adaptées aux besoins et aux capacités de chaque pays participant au projet. Tout en consolidant les acquis du précédent projet CyberSud, CyberSud+ a ajouté les thèmes suivants ou met davantage l'accent sur ceux-ci :

- Cadre légal : soutien à la réforme de la législation nationale, non seulement conformément à la Convention sur la cybercriminalité, mais aussi à son Deuxième Protocole additionnel sur les preuves électroniques, y compris ses normes en matière d'État de droit et de protection des données.
- Capacités d'enquête, de poursuite et de jugement des infractions pénales : Soutien à des programmes de formation durables en matière de cybercriminalité et de preuves électroniques, ainsi qu'à des cours de formation spécialisés, notamment en criminalistique numérique.
- Coopération internationale : soutien à l'élaboration de guides pratiques, de procédures et de modèles, ainsi qu'à des activités de formation nationales et régionales en vue d'une coopération transfrontalière entre gouvernements et entre gouvernements et secteur privé, sur la base des outils du Deuxième Protocole additionnel.
- Synergies entre les réponses de la justice pénale et de la cybersécurité aux cybermenaces : mécanismes de coopération et de communication fiables entre les institutions de cybersécurité et les autorités de justice pénale. Ce volet met l'accent sur les liens entre les mesures relatives à la cybercriminalité et à la cybersécurité.

De plus, le champ d'action du projet a été élargi. Tandis que l'Algérie, la Jordanie, le Liban, le Maroc et la Tunisie restent des pays prioritaires, CyberSud+ coopère également avec l'Égypte, la Libye et la Palestine* dans le cadre des activités du projet et partage ainsi l'expérience acquise jusqu'à présent dans le cadre de CyberSud, par le biais d'activités régionales et, dans la mesure du possible, spécifiques à chaque pays.

relatives au trafic ; la divulgation accélérée de données et la coopération en cas d'urgence ; les équipes d'enquête conjointes et les enquêtes conjointes ; la vidéoconférence. Ces outils sont étayés par des mesures de protection des données et d'autres garanties qui doivent être mises en œuvre par les Parties.

Résultats et produits attendus

Impact	Réduire la vulnérabilité des pays du Sud de la Méditerranée face aux cybermenaces.
Résultat	Meilleures prévention et réponse à la cybercriminalité par les institutions publiques des pays du Sud de la Méditerranée en coopération avec le secteur privé et conformément à la Convention de Budapest.
Livrable 1	Renforcement des capacités des autorités compétentes à introduire des réformes réglementaires et techniques dans les domaines de la cybercriminalité, de la preuve électronique et de la réponse de la justice pénale.
Livrable 2	Amélioration des connaissances et de la spécialisation des professionnels de la justice pénale pour prévenir et combattre la cybercriminalité.
Livrable 3	Accroissement des possibilités de coopération internationale dans le cadre de la Convention de Budapest et de son Deuxième Protocole additionnel.
Livrable 4	Amélioration des procédures et des outils reliant les autorités de justice pénale et les organisations de cybersécurité.

Contact

Virgil Spiridon virgil.spiridon@coe.int
Chef du Bureau des Programmes sur la +40212017810
Cybercriminalité
Conseil de l'Europe