CyberSud
Coopération en matière de lutte contre la cybercriminalité dans le Voisinage Sud

Concept du projet[1]

Version du 02 avril 2020

Titre du projet / numéro (2017/DG1/JP/3692) :	CyberSouth – Coopération en matière de lutte contre la cybercriminalité dans le voisinage sud
Zone du projet :	Région du voisinage sud[2]
	Zones prioritaires initiales : Algérie, Jordanie, Liban, Maroc et Tunisie
Durée :	54 mois (juin 2017 – décembre 2021)
Budget :	5 005 000 EUR
Financement :	Union européenne et Conseil de l'Europe
Mise en œuvre :	Bureau de programme du Conseil de l'Europe sur la cybercriminalité (C-PROC)

CONTEXTE ET JUSTIFICATION

Dans le monde entier, les sociétés s'appuient de plus en plus sur les technologies de l'information et de la communication (TIC) ce qui les rend également vulnérables à diverses menaces comme la cybercriminalité : un terme recouvrant les infractions commises contre des systèmes informatiques au moyen d'ordinateurs. La cybercriminalité affecte aussi bien des individus, des institutions ou des organisations que des États. En outre, les preuves de la commission d'une quelconque infraction sont désormais stockées sur des systèmes informatiques. L'accès à des preuves volatiles sur des ordinateurs et la sécurisation de ces données constituent une tâche complexe, que le stockage soit effectué sur le territoire national ou bien sur des serveurs sur le nuage.

Ce constat s'applique aussi aux pays du voisinage sud. La sécurisation, la fiabilité et la crédibilité des TIC sont indispensables pour permettre à ces sociétés d'exploiter le potentiel de développement humain de ces technologies.

Les gouvernements considèrent de plus en plus la cybercriminalité et la cybersécurité comme des questions relevant de la sécurité nationale, au vu notamment de l'utilisation terroriste d'internet, des activités relevant de la criminalité organisée dans le cyberespace et de rapports faisant état d'attaques et d'intrusions menées par des États ou des acteurs soutenus par des États. Dans certains pays, ces menaces pourraient déclencher des mesures répressives qui, à leur tour, pourraient menacer l'État de droit et les droits de l'homme. Il est par conséquent indispensable de réconcilier l'obligation positive des gouvernements de protéger la société et les individus contre le crime d'une part et le respect de la suprématie du droit, des droits de l'homme et des exigences liées à la protection des données d'autre part.

[1] Le présent résumé a été mis à jour suite à l'extension du projet accordée par la Commission Européenne.

[2] Les 10 pays suivants participent à la Politique européenne de voisinage de l'Union européenne : Algérie, Égypte, Israël, Jordanie, Liban, Libye, Maroc, Palestine*, Syrie et Tunisie.

(*Cette désignation ne saurait être interprétée comme une reconnaissance de l'État de Palestine ni préjuger des positions individuelles des états membres sur la question).

L'approche du Conseil de l'Europe en matière de lutte contre la cybercriminalité vise à relever ce défi. Elle se fonde sur la Convention de Budapest sur la cybercriminalité et des instruments connexes comme la Convention 108 sur la protection des données. L'adhésion à la Convention de Budapest donne droit à un siège au sein du Comité de la Convention sur la cybercriminalité (T-CY) et permet une coopération avec les 68 États déjà parties à cet instrument. De plus, la mise en œuvre de la Convention de Budapest et le travail du T-CY bénéficient de programmes de renforcement des capacités.

La Convention de Budapest est ouverte à tous les pays disposés à appliquer ces dispositions et à s'engager dans la voie de la coopération. Parmi les États du voisinage sud, Israël et Maroc sont Etats partie. Le Maroc est un pays prioritaire du projet conjoint GLACY+ d'action globale sur la cybercriminalité élargie. La Tunisie a exprimé l'intérêt pour la Convention. Le Maroc et la Tunisie sont de plus parties à la Convention 108 du Conseil de l'Europe sur la protection des données.

Dans le cadre d'une approche par phases, l'Algérie, la Jordanie, Liban, le Maroc et la Tunisie seraient considérés comme des pays prioritaires habilités à bénéficier de la gamme complète des services de soutien proposés dans le cadre du présent projet, tandis que la coopération avec les autres pays se concentrerait dans un premier temps sur le renforcement des conditions – liées à la législation et à l'État de droit – propices à la lutte contre la cybercriminalité et à la protection des preuves électroniques, avec l'espoir de les associer ensuite progressivement, si possible, à d'autres activités.

Le Maroc était prioritaire dans le cadre du projet GLACY (2013-2016) et il constitue toujours un pays prioritaire et central dans le cadre du projet GLACY+ (2016-2019). GLACY a déjà permis de constater la faisabilité d'activités de renforcement des capacités en matière de législation relative à la cybercriminalité, de formation des juges à la lutte contre la cybercriminalité et à l'utilisation de preuves électroniques, à la formation des autorités répressives et à la coopération à la fois entre les secteurs public et privé et entre les pays. Les outils et le matériel utilisé dans ce contexte devraient être adaptés à l'utilisation par d'autres pays de la région.

Il est proposé non seulement d'associer le Maroc au projet CyberSouth, mais également de maintenir sa participation à GLACY+. Le Maroc servirait ainsi de lien entre les deux projets et contribuerait au partage de nouveaux outils et pratiques – élaborés dans le cadre de GLACY+ – avec les pays participant à CyberSouth.

De plus, le projet bénéficierait de l'expérience acquise dans le cadre de projets conjoints UE/Conseil de l'Europe menés dans la région du partenariat oriental (Cybercrime@EAP) et dans l'Europe du Sud-Est (iPROCEEDS dans le cadre de l'instrument de préadhésion) en vue d'instaurer une coopération entre les secteurs public et privé et à faciliter la confiscation des produits des crimes en ligne.

OBJECTIF, RESULTATS ATTENDUS ET ACTIVITES

Objectif global	**Contribuer à la prévention et au contrôle de la cybercriminalité et d'autres infractions impliquant la preuve électronique, en conformité aux normes internationales de protection des droits de l'homme et au respect de l'Etat de droit ainsi qu'aux bonnes pratiques.**
Objectif du projet	**Renforcer la législation et les capacités institutionnelles de lutte contre la cybercriminalité et d'utilisation des preuves électroniques dans la région du Voisinage Sud en conformité avec les exigences relatives aux droits de l'homme et à l'État de droit** Au terme du projet : – 2 Etats supplémentaires seront Parties à la Convention de Budapest et 2 autres Etats seront invités à adhérer à la Convention de Budapest. – Les autorités de justice pénale engagent des poursuites en cas d'infractions liées à la cybercriminalité et dans les cas impliquant la preuve électronique et coopèrent au niveau international.
Résultat 1	**Cadres de droit pénal renforcé conformément aux dispositions de la Convention de Budapest sur la cybercriminalité, y compris la règle de respect des sauvegardes prévues par le droit interne (article 15)** Au terme du projet : – Au moins trois pays supplémentaires auront un cadre juridique conforme à la Convention de Budapest. Deux autres pays auront des projets de loi e conformité avec la Convention de Budapest.
Activités :	– Préparer une évaluation (étude) sur la législation relative à la cybercriminalité et à la preuve électronique dans les pays prioritaires et dans d'autres pays du Voisinage Sud, y compris les profils juridiques. – Préparer une évaluation (étude) sur le cadre de la protection des données dans les pays prioritaires. – Organiser des ateliers régionaux sur la législation en matière de cybercriminalité et de protection de données ainsi que sur les statistiques de la justice pénale afin de déterminer l'efficacité de la législation. – Mener des études sur des projets de loi et assurer un suivi avec un atelier dans le pays. – Documenter la jurisprudence concernant la cybercriminalité et la preuve électronique et publier sur Octopus Community. – Soutenir des ateliers dans les pays à destination des juges, procureurs et force de l'ordre sur l'application de la législation en matière de cybercriminalité, y compris les exigences en matière d'Etat de droit et de protection des données. – Soutenir des ateliers dans les pays pour développer des guides sur les conditions et sauvegardes dans les investigations en matière de cybercriminalité et preuves électroniques.
Résultat 2	**Services de police et de poursuites spécialisés et renforcement de la coopération interservices d'une approche soutenable**

	Au terme du projet – Les unités de police spécialisées dans les pays prioritaires sont opérationnelles et exposent une augmentation de 25% des investigations. – Procédures nationales sur les investigations en matière de cybercriminalité et preuves électroniques en place dans tous les pays prioritaires.
Activités:	– Analyse des capacités institutionnelles en matière d'enquêtes et de poursuites visant des actes de cybercriminalité, ainsi que d'investigations informatiques. – Conseil, partage d'expériences et visites d'études concernant l'établissement ou le renforcement de services spécialisés – Soutien au développement de stratégies de formation en cybercriminalité et accès aux matériels de formation. – Soutien au recours à des procédures opérationnelles standards en matière de traitement des preuves électroniques – Promotion de la coopération interservices – entre les unités chargées de la cybercriminalité, les enquêteurs financiers et les cellules de renseignement financier – en matière de recherche, saisie et confiscation des produits des crimes en ligne – Promotion de la coopération entre les secteurs public et privé, en particulier entre les autorités répressives et les fournisseurs de services s'agissant des modalités d'accès aux preuves électroniques – Soutien au développement de Procédures Opérationnels Standard pour la collecte, l'analyse et la présentation des preuves électroniques – Soutien au développement d'une boîte à outils pour les premiers intervenants dans les investigations en matière de la cybercriminalité – Soutien à l'établissement d'un partenariat avec les fournisseurs de services multinationaux.
Résultat 3	**Standardisation de la formation des membres du système judiciaire à la lutte contre la cybercriminalité et au traitement des preuves électroniques** Au terme du projet : – Des modules de formation en cybercriminalité et preuve électronique sont inclus dans les programmes de formation des institutions de formation. – Développement de cours de formation judiciaire nationaux sur la cybercriminalité et les preuves électroniques dans tous les pays prioritaires. – Part des magistrats de référence ayant reçu une formation de base et avancée dispensée par des formateurs locaux.
Activités :	– Préparer une évaluation (étude) sur les systèmes de formation des juges et des capacités dans la région de Voisinage du Sud – Organiser un atelier régional pour les représentants des institutions de formation judiciaire afin de parvenir à un accord sur la démarche à suivre. – Organiser des ateliers de formations aux formateurs (dans cinq pays). – Soutenir l'adaptation des supports de formation (cours de base). – Soutenir la dispense d'un cours de base par des formateurs formés dans les cinq pays. – Organiser une conférence régionale sur les progrès réalisés et sur l'intégration de la formation sur la cybercriminalité et la preuve électronique dans les programmes de formation des institutions de formation. – Soutenir les ateliers nationaux pour le développement des cours de formation judiciaire nationaux sur la cybercriminalité et la preuve électronique.

	– Soutenir la mise en place d'activités de formation dans le pays sur la base des cours de formation judiciaire nationaux et la mise en place d'une formation TOT pour les magistrats de référence.
Résultat 4	**Les autorités de justice pénale disposent de meilleures compétences et de meilleurs outils pour une coopération internationale plus efficace en matière de cybercriminalité et de preuve électronique** Au terme du projet : – Rôle et performance des points de contact 24/7 conformément aux procédures opérationnelles mises en place. À la fin du projet, des points de contact sont établis dans 5 pays prioritaires et envoient et reçoivent des demandes. – Création d'un réseau judiciaire régional (CyberSud).
Activités:	– Préparer une évaluation (étude) sur les autorités compétentes et sur le fonctionnement de la coopération internationale dans la région du Voisinage Sud. – Organiser une conférence régionale/internationale sur les rôles et les responsabilités dans la coopération internationale police à police internationale et judiciaire en matière de cybercriminalité et de preuve électronique. – Effectuer des missions de conseil sur la mise en place des points de contact 24/7 – Organiser des ateliers de formation régionaux sur la coopération internationale et le rôle de 24/7 points de contact (mise au point sur des questions telles que sextortion et d'autres questions d'intérêt commun). – Soutenir la participation des représentants des pays du Voisinage Sud au Comité de la Convention sur la cybercriminalité, aux conférences annuelles de l'EUROPOL/INTERPOL et à d'autres réunions internationales et activités de formation. – Organiser deux conférences régionales/internationales pour soutenir la création et le fonctionnement du réseau judiciaire CyberSud. – Soutenir l'organisation d'un atelier régional/international sur le fonctionnement des différents réseaux et leur utilisation, par exemple sur le réseau de la Convention de Budapest 24/7, le G7 et i24/7 Interpol, et l'élaboration de procédures opérationnelles pour les points de contact 24/7.
Résultat 5	**Les stratégies prioritaires en cybercriminalité et preuve électronique sont identifiées** Au terme du projet – Les priorités stratégiques sont approuvées par les pays prioritaires sur la base d'une évaluation de la législation et des capacités institutionnelles.
Activités :	– Préparer une évaluation (étude) sur les politiques actuelles en cyber sécurité et cybercriminalité ou sur les stratégies dans la région de Voisinage Sud. – Organiser une conférence de lancement sur les stratégies/politiques en cybercriminalité avec la participation de hauts fonctionnaires de la région du Voisinage Sud. – Soutenir l'élaboration de rapports de situation (annuelle) sur la cybercriminalité et la preuve dans les cinq pays prioritaires. – Organiser une conférence nationale sur la cybercriminalité dans cinq pays prioritaires. – Préparer une évaluation (étude) sur les progrès en cours réalisés en ce qui concerne la législation et les capacités institutionnelles depuis le début du projet dans la région du Voisinage Sud.

	– Organiser une conférence de clôture du projet afin d'examiner les progrès accomplis et d'adopter un ensemble de priorités stratégiques.

CONTACT
Alexander Seger
Chef de la division Cybercriminalité, Conseil de l'Europe
alexander.seger@coe.int

www.coe.int/cybercrime

Financé par l'Union européenne et le Conseil de l'Europe

UNION EUROPÉENNE

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Mis en œuvre par le Conseil de l'Europe