COUNCIL OF EUROPE

CONSEIL DE L'EUROPE

Documents d'information

SG/Inf(2026)11

4 mai 2026

Bureau du Programme sur la cybercriminalité du Conseil de l'Europe à Bucarest : Rapport d'activité pour 2025

Contenu

Résumé

Le Bureau du Programme sur la cybercriminalité du Conseil de l'Europe (ci-après dénommé « le Bureau »)[1] à Bucarest, en Roumanie, est chargé de la mise en œuvre de projets de renforcement des capacités en matière de cybercriminalité et de preuves électroniques sur la base de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest, STE n° 185). Le Bureau est devenu opérationnel en 2014 à la suite d'une décision du Comité des Ministres en 2013. Cette décision prévoyait également que le Secrétaire Général présente chaque année un rapport au Comité des Ministres.

En 2025, le Bureau a consolidé sa position en tant que pilier du renforcement des capacités, de l'harmonisation législative et de la coordination des parties prenantes dans la lutte contre la cybercriminalité à l'échelle mondiale. Grâce à sept projets internationaux en cours, le Bureau a mené 294 activités, touchant les acteurs de la justice pénale dans le monde entier.

Cet engagement de grande envergure a conduit à une augmentation significative du nombre d'enquêteurs, de procureurs et de juges qui sont désormais mieux formés et équipés pour traiter la cybercriminalité et les preuves électroniques. En conséquence, l'état de droit et l'efficacité des réponses pénales ont été directement renforcés dans de nombreux États membres et pays partenaires.

Depuis sa création, le Bureau a soutenu environ 2700 activités, dont ont bénéficié quelque 140 pays. En décembre 2025, il comptait 47 employés, y compris le personnel d'autres bureaux du Conseil de l'Europe, notamment à Kyiv et à Pristina.

Le renforcement des capacités a soutenu les efforts déployés aux niveaux national, régional et mondial, conformément à la Déclaration de Reykjavík du Conseil de l'Europe, en étendant les normes et les bonnes pratiques de l'organisation bien au-delà de l'Europe.

Le travail du Bureau a également eu un impact législatif direct : en décembre 2025, 134 États avaient mis à jour leur législation nationale afin de criminaliser les infractions commises contre et au moyen d'ordinateurs, conformément à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), contre seulement 70 États en 2013.

Le nombre d'États participant au cadre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) continue d'augmenter, avec 97 États étant soit parties (81), signataires (2) ou invités à adhérer (14) en janvier 2026, soit près du double de la participation depuis 2013.

1. Pour la période d'avril 2014 à septembre 2015, voir ce rapport (disponible en anglais uniquement).
Pour la période d'octobre 2015 à septembre 2016, voir ce rapport (disponible en anglais uniquement).
Pour la période d'octobre 2016 à septembre 2017, voir ce rapport.
Pour la période d'octobre 2017 à septembre 2018, voir ce rapport.
Pour la période d'octobre 2018 à septembre 2019, voir ce rapport.
Pour la période d'octobre 2019 à septembre 2020, voir ce rapport.
Pour la période d'octobre 2020 à septembre 2021, voir ce rapport.
Pour la période d'octobre 2021 à décembre 2022, voir ce rapport.
Pour la période de janvier à décembre 2023, voir ce rapport.
Pour la période allant de janvier à décembre 2024, voir ce rapport.

Le Bureau a également facilité le processus de signature du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) relatif au renforcement de la coopération et de la divulgation de preuves électroniques, qui, en janvier 2026, avait été signé par 52 États (dont 2 ratifications), soulignant le rôle clé joué par le Bureau pour assurer des cadres juridiques à jour face aux évolutions technologiques.

Le Bureau a notamment élargi sa couverture thématique du renforcement des capacités en abordant de nouveaux sujets en 2025, tels que la protection des enfants en ligne, les mesures contre la diffusion non consentie d'images intimes, l'interaction entre les actifs virtuels et la cybercriminalité, ainsi que les implications de l'intelligence artificielle pour le travail de la justice pénale.

L'une des réalisations marquantes de 2025 a été le travail du Bureau avec les académies de formation afin de garantir la scalabilité des compétences récemment acquises en intégrant des modules sur la cybercriminalité et les enquêtes sur les preuves électroniques dans les programmes nationaux de formation destinés aux enquêteurs, aux procureurs et aux juges.

Fondamentalement, le Bureau a développé des partenariats et des synergies avec d'autres organisations internationales et régionales telles que le Réseau des responsables juridiques des îles du Pacifique (Pacific Islands Law Officers Network, PILON), le Centre de Capacités Cyber des Balkans occidentaux (Western Balkans Cyber Capacity Centre, WB3C), l'Agence de l'Union européenne pour la coopération en matière de justice pénale (Eurojust), l'Agence de l'Union européenne pour la coopération des services répressifs (Europol), l'Agence de l'Union européenne pour la formation des services répressifs (CEPOL), le Groupe européen pour la formation et l'éducation en matière de cybercriminalité (European Cybercrime Training and Education Group, ECTEG), le Forum mondial de l'expertise cybernétique (Global Forum for Cyber Expertise, GFCE), l'Organisation des États américains (Organisation of American States, OEA), l'Office des Nations Unies contre la drogue et le crime (ONUDC), INTERPOL[2], la Communauté des Caraïbes (CARICOM), l'Organisation des États de la Caraïbe orientale (OECO) et l'Organisation pour la sécurité et la coopération en Europe (OSCE), maximisant ainsi l'impact du projet et l'efficacité de l'utilisation des ressources à l'échelle mondiale.

Le Bureau a maintenu et renforcé son rôle central au sein de la « triade dynamique » composée de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), de son Comité de la Convention sur la cybercriminalité et du Bureau lui-même, garantissant ainsi le maintien du leadership et de la capacité d'innovation du Conseil de l'Europe dans ce domaine.

En élargissant sa portée mondiale, en s'adaptant aux nouveaux défis et en renforçant sa collaboration avec les principales parties prenantes et les organisations internationales, en 2025 le Bureau a réalisé des progrès significatifs et innovants, jetant ainsi des bases solides pour un impact encore plus important dans les années à venir.

Le Bureau a également continué à jouer un rôle déterminant dans les travaux du Comité de la Convention sur la cybercriminalité, en soutenant l'élaboration de lignes directrices pratiques à l'intention des Parties, en cofinançant et en coorganisant des réunions plénières clés, et en assurant le fonctionnement efficace du réseau 24/7, un outil essentiel pour la coopération internationale dans les affaires de cybercriminalité.

2. Le Complexe mondial INTERPOL pour l'innovation (IGCI) à Singapour est partenaire du projet GLACY-e sur le renforcement de l'action mondiale contre la cybercriminalité. Dans le cadre d'un accord de subvention, INTERPOL est responsable du volet « application de la loi » de ce projet.

Afin de garantir que le Bureau reste un leader mondial en matière de renforcement des capacités dans le domaine de la cybercriminalité, les priorités clés suivantes se dégagent de ses récentes réalisations et de l'évolution du contexte international :

- Préserver et renforcer sa capacité à opérer à l'échelle nationale, régionale et mondiale, en étendant les normes du Conseil de l'Europe à de nouvelles juridictions et en tirant parti de déclarations multilatérales telles que la Déclaration de Reykjavík afin d'étendre son influence bien au-delà de l'Europe.

- Aider davantage d'États à aligner leur législation nationale en matière de cybercriminalité et de preuves électroniques sur la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), dans le but d'augmenter encore le nombre d'États qui adoptent et mettent en œuvre efficacement ses dispositions et protocoles additionnels**.**

- Accélérer la promotion, la signature, la ratification et la mise en œuvre effective du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) par un groupe plus large d'États, en facilitant l'accès transfrontalier aux preuves électroniques dans un environnement technologique dynamique et en constante évolution.

- Rester proactif en intégrant les nouveaux thèmes prioritaires dans les programmes de formation et l'assistance technique – tels que la cyberviolence, la désinformation, la protection des enfants en ligne, l'utilisation abusive des actifs virtuels, l'intelligence artificielle et l'ingérence électorale – afin de suivre l'évolution du paysage de la criminalité numérique.

- Mobiliser des fonds supplémentaires, encourager les contributions volontaires et assurer la viabilité opérationnelle et administrative du Bureau, afin de lui permettre de lancer de nouveaux projets et d'étendre ses activités en fonction des besoins et en réponse à la demande mondiale.

En poursuivant ces priorités, le Bureau pourra maintenir sa position à l'avant-garde de la lutte mondiale contre la cybercriminalité, en promouvant des normes, en renforçant les capacités et en consolidant la coopération internationale pour la prochaine décennie et au-delà.

1. Contexte et objectif du présent rapport

Le présent rapport a pour objectif d'informer le Comité des Ministres des activités menées en 2025 par le Bureau du Programme sur la cybercriminalité du Conseil de l'Europe (ci-après dénommé « le Bureau ») à Bucarest, en Roumanie.

Le Bureau est devenu opérationnel en avril 2014 à la suite d'une offre du gouvernement roumain[3] et d'une décision du Comité des Ministres en octobre 2013.[4] Son objectif est d'assurer la mise en œuvre des projets de renforcement des capacités du Conseil de l'Europe en matière de cybercriminalité dans toutes les régions du monde.

3. Le Bureau est situé à la Maison des Nations Unies à Bucarest. Les locaux sont mis à la disposition du Conseil de l'Europe gratuitement par le gouvernement roumain dans le cadre d'un protocole d'accord.
4. Décisions CM/Del/Dec(2013)1180/10.4, 9 octobre 2013, lors de leur 1180e réunion.

Faisant le point sur l'expérience acquise par le Bureau depuis plus de 11 ans, l'adhésion croissante à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), les synergies avec la Convention des Nations Unies contre la cybercriminalité[5], les demandes croissantes en matière de renforcement des capacités et les nouveaux domaines d'impact (intelligence artificielle, actifs virtuels, cyberviolence et désinformation), le présent rapport réfléchit également aux priorités futures.

2. Contexte général

Le Bureau joue un rôle essentiel à une époque où la cybercriminalité évolue rapidement. Son ampleur, sa sophistication et sa diversification dépassant constamment les capacités nationales en matière d'application de la loi, mettant en évidence les lacunes des réponses mondiales. Cela souligne la nécessité d'une assistance technique au niveau mondial pour aider les pays à élaborer, mettre en œuvre et appliquer des stratégies, des législations et des compétences opérationnelles efficaces en matière de cybercriminalité et de preuves électroniques.

Au niveau international, l'adoption de la Convention des Nations Unies contre la cybercriminalité marque un tournant décisif, où les pays reconnaissent la nécessité d'harmoniser les réponses mondiales et à renforcer la coopération en matière d'enquête et de poursuite des crimes commis au moyen des systèmes de technologie de l'information et de la communication.

Parallèlement, le Bureau continue de jouer un rôle déterminant dans le soutien à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), la principale norme internationale dans ce domaine, et à promouvoir la mise en œuvre de son Deuxième Protocole additionnel, qui améliore l'accès transfrontalier aux preuves électroniques.

Le travail du Bureau à ce carrefour garantit la mise en place des compétences pratiques et des outils juridiques nécessaires pour aider les États à répondre de manière décisive aux défis posés par la criminalité numérique et les preuves électroniques dans un monde complexe et interconnecté.

Paysage de la cybercriminalité

La cybercriminalité représente l'une des catégories d'activités criminelles qui connaît la croissance la plus rapide et la plus complexe, posant des défis importants aux autorités judiciaires pénales du monde entier.

Les infractions sont de plus en plus transnationales, sophistiquées sur le plan technologique et hautement adaptables, exploitant les lacunes juridiques, techniques et juridictionnelles.

Les menaces les plus courantes en matière de cybercriminalité comprennent la fraude en ligne, l'ingénierie sociale, les ransomwares, l'extorsion par voie électronique et l'usurpation d'identité. Ces actes sont le fait à la fois de particuliers et d'organisations criminelles transnationales. Le phishing, le piratage des e-mails professionnels et les escroqueries à l'investissement restent parmi les infractions les plus courantes et les plus préjudiciables sur le plan financier, reposant souvent sur la manipulation psychologique plutôt que sur des compétences techniques avancées. Les attaques par ransomwares continuent de cibler les institutions publiques, les prestataires de soins de santé et les infrastructures critiques, combinant le chiffrement des systèmes et la fuite de données pour accroître la pression sur les victimes.

5. Doc. ONU A/RES/79/243.

Parallèlement, les identifiants et les données personnelles volés sont vendus sur des marchés illicites en ligne, ce qui favorise la poursuite des activités criminelles. Les menaces émergentes, notamment l'utilisation criminelle de l'intelligence artificielle, des deepfakes et des technologies d'anonymisation, compliquent encore davantage la détection, l'attribution et la collecte de preuves.

Pour lutter efficacement contre la cybercriminalité, il faut des cadres juridiques clairs, harmonisés et neutres sur le plan technologique. Les autorités judiciaires pénales ont besoin d'une législation qui criminalise de manière adéquate les infractions dépendantes ou facilitées par le cyberespace, permette l'accès légal aux preuves électroniques et soutienne la coopération transfrontalière. Les lois procédurales doivent suivre le rythme des évolutions technologiques et traiter des questions telles que la conservation des données, le cryptage, les preuves basées sur le cloud et le rôle des prestataires de services privés. L'harmonisation internationale est particulièrement importante, car les délinquants opèrent régulièrement dans plusieurs juridictions, tandis que les enquêtes restent limitées par les frontières juridiques nationales.

Au-delà de la législation, les acteurs de la justice pénale ont besoin d'une assistance technique et d'un renforcement des capacités soutenus. Cela comprend une formation spécialisée pour les enquêteurs, les procureurs et les juges, l'accès à des outils modernes de criminalistique numérique et des mécanismes institutionnels de coopération avec les experts en cybersécurité et le secteur privé. Il est essentiel de renforcer les capacités opérationnelles et la compréhension juridique afin de combler les lacunes en matière d'application de la loi, d'améliorer les résultats des poursuites et de garantir que les réponses à la cybercriminalité respectent les procédures régulières et les droits fondamentaux.

Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest)

La Convention du Conseil de l’Europe sur la cybercriminalité (Convention de Budapest) constitue le premier cadre juridique international complet visant à harmoniser les lois sur la cybercriminalité, à améliorer la coopération en matière d'enquêtes et à permettre une action transfrontalière efficace contre les crimes commis via des systèmes informatiques.

La Convention constitue depuis plus de 20 ans une base solide pour le renforcement des capacités mené par le Conseil de l'Europe, en offrant des orientations et un modèle juridique commun qui aide les États à élaborer une législation en matière de cybercriminalité ainsi que des mécanismes de coopération internationale au-delà de l'Europe.

La tendance à l'accélération de l'intérêt pour la Convention du Conseil de l’Europe sur la cybercriminalité (Convention de Budapest) s'est poursuivie en 2025, lorsque le Rwanda, Sao Tomé-et-Principe, le Vanuatu et la Nouvelle-Zélande sont devenus parties à la Convention, portant le nombre de parties à 81. En outre, les Seychelles, la Malaisie ainsi qu'Antigua-et-Barbuda ont été invitées à y adhérer.

Par ailleurs, Malte a ratifié et le Rwanda a adhéré au Premier Protocole additionnel à la Convention du Conseil de l’Europe sur la cybercriminalité (Convention de Budapest) en 2025, ce qui témoigne de l'intérêt croissant pour le cadre de la Convention.

Ces adhésions, ainsi que les demandes d'adhésion, ont été précédées par le soutien du Bureau, en particulier en matière de réforme de la législation nationale. Le Bureau accordant la priorité à une assistance allant au-delà du cadre législatif pour les pays parties ou invités à adhérer, le nombre de pays nécessitant un soutien plus important ne cesse d'augmenter.

Outre le renforcement des capacités, l'intérêt croissant pour la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) depuis 2022 semble principalement dû à deux autres facteurs :

- L'ouverture à la signature du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest, STCE n° 224) en mai 2022.

- La Convention des Nations Unies contre la cybercriminalité adoptée par l'Assemblée générale des Nations Unies le 24 décembre 2024[6].

Deuxième Protocole additionnel à la Convention sur la cybercriminalité

Le Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) vise à renforcer la coopération internationale en permettant un accès plus rapide et plus efficace aux preuves électroniques au-delà des frontières, ce qui est essentiel pour enquêter sur la cybercriminalité moderne. Il renforce également le soutien apporté aux pays en fournissant des outils pratiques, des garanties en matière de droits de l'homme et des procédures plus claires qui aident les États à répondre à la cybercriminalité de manière rapide et coordonnée. Des outils innovants, notamment ceux qui concernent la coopération directe avec les fournisseurs de services dans d'autres parties et la coopération dans les situations d'urgence, sont indispensables aux praticiens de la justice pénale.

Le Protocole est en synergie avec le cadre réglementaire de l'UE sur les preuves électroniques[7] en utilisant des procédures harmonisées pour la demande et la divulgation de preuves électroniques, de sorte que les autorités de l'UE peuvent s'appuyer sur le cadre européen en matière de preuves électroniques au sein de l'Union européenne tout en utilisant le protocole pour coopérer efficacement avec les pays tiers, garantissant ainsi la cohérence, la rapidité et les garanties entre les juridictions.

En décembre 2025, ce protocole avait été ratifié par deux pays (la Serbie et le Japon) et signé par 50 autres États[8]. Les nouveaux pays signataires en 2025 sont la Lettonie, les Fidji, la Norvège, ainsi que la Bosnie-Herzégovine. Cinq ratifications sont nécessaires pour son entrée en vigueur.

6. Le titre complet de ce traité, tel qu'adopté par l'Assemblée générale des Nations Unies (AGNU) en décembre 2024, est « Convention des Nations Unies contre la cybercriminalité ; renforcement de la coopération internationale pour lutter contre certaines infractions commises au moyen de systèmes d''information et de communication et pour la communication de preuves sous forme électronique d'infractions graves ».
7. Règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux ordonnances européennes de production et de conservation de preuves électroniques dans le cadre de procédures pénales et de l'exécution des peines privatives de liberté à la suite de procédures pénales, et directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées relatives à la désignation d'établissements désignés et à la nomination de représentants légaux aux fins de la collecte de preuves électroniques dans le cadre de procédures pénales.
8. La Hongrie et le Costa Rica ont ratifié le deuxième protocole additionnel le 5 février 2026 et le 15 avril 2026 respectivement, portant ainsi à quatre le nombre de ratifications. Ces ratifications ne sont toutefois pas intervenues pendant la période couverte par le présent rapport d'activité.

Le Bureau a soutenu la promotion et la mise en œuvre du Deuxième Protocole additionnel en fournissant une assistance technique, des conseils juridiques et des activités de renforcement des capacités, telles que des formations, des ateliers et un soutien législatif, afin d'aider les pays à comprendre les mécanismes du protocole, à aligner leurs lois nationales et à appliquer efficacement ses procédures dans la pratique.

La mise en œuvre et la ratification du Protocole resteront une priorité pour le Bureau dans les années à venir.

Comité de la Convention sur la cybercriminalité

Le Comité de la Convention sur la cybercriminalité a pour objectif de garantir la mise en œuvre effective et la pertinence continue de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) en guidant les parties à travers l'élaboration de politiques, des évaluations, des mécanismes de coopération et l'engagement avec les principales parties prenantes.

En 2025, le Comité de la Convention sur la cybercriminalité a continué à jouer un rôle central dans l'orientation de la mise en œuvre de la Convention. Parmi les principales réalisations figurent l'adoption, en juin, d'une note d'orientation sur l'article 26 relatif aux informations spontanées, ainsi que le lancement d'un questionnaire sur la cyberviolence visant à soutenir la mise à jour de la ressource sur la cyberviolence.

Le Comité de la Convention sur la cybercriminalité a également fait progresser ses travaux analytiques en créant un groupe de travail sur l'intelligence artificielle et en lançant une étude cartographique sur les actifs virtuels et leur pertinence pour la Convention.

Parallèlement, le Comité de la Convention sur la cybercriminalité a renforcé la coopération internationale grâce à des réunions avec l'industrie et les fournisseurs de services.

La participation de nombreux experts aux plénières du Comité de la Convention sur la cybercriminalité en juin et novembre 2025 a été financée par des projets mis en œuvre par le Bureau.

Le Bureau assure également le fonctionnement du réseau 24/7 (créé conformément à l'article 35 de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et organise les réunions annuelles du réseau.

Le Bureau continuera à soutenir le Comité de la Convention sur la cybercriminalité dans ces efforts. Ces thèmes deviendront des éléments importants des activités de renforcement des capacités.

Convention des Nations Unies contre la cybercriminalité

Le lancement de la Convention des Nations Unies contre la cybercriminalité en octobre 2025 a marqué l'aboutissement du processus du Comité ad hoc des Nations Unies, qui a tenu huit sessions entre février 2022 et août 2024, alternativement à New York et à Vienne.

Ce lancement reflétait l'engagement commun des États à renforcer la coopération internationale et à harmoniser les réponses à la cybercriminalité au niveau mondial. Il soulignait également l'importance d'assurer la cohérence avec les instruments et pratiques existants développés dans le cadre des cadres établis en matière de

cybercriminalité. À la fin de 2025, la Convention des Nations Unies comptait 74 signataires.

Le Conseil de l'Europe a contribué à ce processus de négociation du traité par le biais du Comité de la Convention sur la cybercriminalité (sous la forme de notes d'information) et du Bureau, en soutenant la participation d'experts en la matière issus des parties à la Convention et des États invités à y adhérer à chaque session. L'objectif était de garantir la cohérence de ce traité supplémentaire avec la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et l'inclusion des garanties minimales en matière de droits humains et d'État de droit nécessaires à la coopération internationale.

Ces résultats ont été atteints : la Convention des Nations Unies contre la cybercriminalité comprend en grande partie des dispositions adaptées de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), de la Convention des Nations Unies contre la criminalité transnationale organisée (UNTOC) et de la Convention des Nations Unies contre la corruption (UNCAC.)[9]

Toutefois, des défis subsistent en ce qui concerne la mise en œuvre effective de ses conditions et garanties. Pour la prochaine période, il est essentiel que les États mettent en œuvre la nouvelle Convention des Nations Unies d'une manière compatible avec la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), ce qui peut être réalisé grâce à des activités conjointes de renforcement des capacités impliquant le Bureau du Conseil de l'Europe et l'ONUDC.

Les partenariats liés aux deux conventions peuvent prendre la forme d'une coopération visant à soutenir leur mise en œuvre complémentaire, d'outils d'enquête liés à l'exploitation et aux abus sexuels des enfants en ligne et le renforcement des capacités avec des garanties solides en matière de droits humains et d'État de droit, tout en apportant une expertise au processus en cours au sein des Nations Unies.

3. Aperçu des projets et des réalisations en 2025

Projets

En 2025, le Bureau comptait six projets régionaux et mondiaux et un projet spécifique à un pays (Ukraine) en cours de mise en œuvre. En décembre 2025, le budget combiné des projets en cours s'élevait à quelque 40,8 millions d'euros.

Titre du projet	Durée	Budget	Financement
Octopus Projet visant à soutenir la mise en œuvre de la Convention sur la cybercriminalité, de ses protocoles et des normes connexes à l'échelle mondiale	Janvier 2021 – décembre 2027	10 millions d'euros	Contributions volontaires (Canada, France, Hongrie, Islande, Italie, Japon, Pays-Bas, Malte, Royaume-Uni et États-Unis[10]) [financement non entièrement garanti]
Projet GLACY-e sur le renforcement de l'action mondiale contre la cybercriminalité	Août 2023 – décembre 2028	13,25 millions d'euros	Projet conjoint UE/CoE (dont 10 % CoE OB/JPP)

9. En ce qui concerne les liens entre les deux conventions, voir : https://rm.coe.int/conventions-on-cybercrime-the-budapest-convention-and-the-draft-un-tre/1680b1631a (disponible en anglais uniquement).
10. Voir également la note de bas de page n° 12.

Projet CyberUA sur le renforcement des capacités en matière de preuves électroniques des crimes de guerre et des violations flagrantes des droits humains en Ukraine	Février 2024 – décembre 2026	2 millions d'euros	Contributions volontaires au plan d'action pour l'Ukraine[11] et OBC [financement non entièrement garanti]
CyberEast+ sur le renforcement de la lutte contre la cybercriminalité pour la cyber-résilience dans les États du Partenariat oriental	Mars 2024 – février 2027	3,89 millions d'euros	Projet conjoint UE/CoE (dont 10 % CoE OB/JPP)
Projet CyberSouth+ sur le renforcement de la coopération en matière de cybercriminalité et de preuves électroniques dans la région du voisinage méridional	Janvier 2024 – décembre 2026	3,89 millions d'euros	Projet conjoint UE/CoE (dont 10 % CoE OB/JPP)
Projet CyberSEE sur le renforcement de la lutte contre la cybercriminalité et les preuves électroniques en Europe du Sud-Est et en Türkiye	Janvier 2024 – juin 2027	5,55 millions d'euros	Projet conjoint UE/CoE (dont 10 % CoE OB/JPP)
Projet CyberSPEX sur le renforcement de la coopération entre les États membres de l'UE en matière de preuves électroniques par le biais du deuxième protocole additionnel à la convention sur la cybercriminalité	Mars 2024 – décembre 2026	2,23 millions d'euros	Projet conjoint UE/CoE (dont 10 % CoE OB/JPP)

Les projets mis en œuvre par le Bureau reposent principalement sur des financements externes, comme le montre le tableau ci-dessus. Néanmoins, les projets conjoints avec l'UE bénéficient d'un cofinancement à hauteur de 10 % provenant du programme commun du budget ordinaire du Conseil de l'Europe.

L'UE est restée le principal donateur dans le cadre des projets conjoints cofinancés par le Conseil de l'Europe. Les États-Unis ont par le passé apporté un financement important au projet Octopus[12].

Toutefois, la poursuite du projet Octopus, qui est également pertinent pour le fonctionnement du Comité de la Convention sur la cybercriminalité, n'est actuellement pas assurée. Il convient donc de s'efforcer à l'avenir de lever des fonds supplémentaires afin de garantir la poursuite, au-delà de 2026, du travail vital accompli dans le cadre de ce projet.

Le Bureau compte également sur le soutien du gouvernement roumain, qui continue de lui fournir des locaux gratuitement.

En 2025, des progrès importants ont été réalisés en ce qui concerne la poursuite des projets existants, puisque le projet GLACY-e a été prolongé pour la période 2026-2028 avec un budget supplémentaire de 7,7 millions d'euros. Les projets CyberSPEX et CyberUA ont été prolongés sans frais jusqu'à la fin de 2026.

11. Plan d'action du Conseil de l'Europe pour l'Ukraine « Résilience, relèvement et reconstruction » (2023-2026).
12. Remarque : le Conseil de l'Europe a été informé par les autorités américaines le 28 janvier 2025 que le financement reçu des États-Unis allait être « suspendu ». Le 13 mars 2025, le Conseil de l'Europe a ensuite été informé que la suspension avait été levée.

En outre, la préparation du projet GlacyFOA a commencé et devrait être signée au cours du premier trimestre 2026. Cette action est une initiative conjointe de l'UE et du Conseil de l'Europe visant à lutter contre la fraude en ligne dans les pays d'Afrique de l'Ouest.

Tout au long de l'année, le Bureau a soutenu, avec quelque 47 collaborateurs, plus de 294 activités dans le cadre de ces projets. Un inventaire détaillé de toutes les activités menées depuis 2014 est disponible en ligne.

Réalisations

Capacités en matière de justice pénale

En 2025, le C-PROC a contribué de manière significative au renforcement des capacités en matière de justice pénale, en particulier dans les quelque 50 pays prioritaires qui pouvaient bénéficier d'une large gamme d'aides. Quelque 90 autres pays ont participé à au moins certaines des activités.

Voici quelques exemples d'activités spécifiques et de résultats obtenus dans le cadre de différents projets :

- Dans le cadre du projet **CyberEast+** sur le renforcement de la lutte contre la cybercriminalité et pour la cyber-résilience dans les États du Partenariat oriental :

  La mise en œuvre du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) est restée un élément clé de l'action du projet en 2025, avec un mélange d'activités nationales traitant des aspects juridiques de la mise en œuvre et de la coopération public-privé du traité, et la réunion régionale traitant de la conformité avec les exigences de l'UE en ce qui concerne le protocole.

  Les actions de formation et de renforcement des capacités avec les services répressifs et judiciaires ont été particulièrement variées en 2025, abordant des thèmes tels que les monnaies virtuelles et les enquêtes sur le darknet, les enquêtes sur les ransomwares à travers des exercices nationaux, les enquêtes sur les logiciels malveillants et les réseaux, les enquêtes sur la maltraitance des enfants à l'aide de renseignements open source, la désinformation criminelle, les attaques contre le secteur de l'énergie et d'autres domaines. Un cyber exercice régional annuel hautement technique et un exercice bilatéral de suivi avec des partenaires ukrainiens ont permis de mettre l'accent sur les thèmes de la cyber-ingérence dans les élections et des opérations de désinformation.

  Le projet a également travaillé en parallèle à l'amélioration des programmes de formation sur la cybercriminalité et les preuves électroniques, tant au niveau régional que bilatéral. D'autres possibilités de formation ont été explorées lors d'une réunion régionale sur l'utilisation de l'IA dans les enquêtes et la criminalistique, ainsi que dans le cadre de discussions bilatérales avec des avocats de la défense et des associations du barreau.

  La coopération interinstitutionnelle comprend une série d'actions bilatérales avec les pays, axées sur des outils et des procédures compatibles, conformément aux procédures opérationnelles standard convenues, ainsi que sur l'interopérabilité des systèmes de signalement. La coopération transfrontalière s'est appuyée sur des activités conjointes avec les partenaires du projet et les agences de l'UE, l'accent étant mis sur le Deuxième protocole additionnel et la coopération en matière répressive.

L'engagement et la sensibilisation de la société civile ont été renforcés par le soutien annuel continu au dialogue européen sur la gouvernance de l'internet (EuroDIG 2025) au niveau régional et par des sessions consacrées à la cyberviolence dans les pays participant au projet, auxquelles ont pris part des acteurs de la société civile.

Le projet a soutenu 47 activités au cours de cette période.

- Dans le cadre du projet **CyberUA** visant à renforcer les capacités en matière de preuves électroniques des crimes de guerre et des violations graves des droits humains en Ukraine :

  Les processus à long terme visant à améliorer la législation et la coopération internationale en matière de données et de preuves relatives aux crimes de guerre et aux violations flagrantes des droits de l'homme (en particulier la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et de son deuxième protocole additionnel) ont été au centre du soutien continu apporté par le projet. Les autorités sont restées étroitement associées au projet dans le cadre de ces travaux.

  Les compétences et les capacités des autorités pénales ont été améliorées grâce à des sessions de formation spécialisées et des exercices pratiques. Le projet a couvert à la fois les besoins fondamentaux/initiaux (recevabilité, renseignement d'origine sources ouvertes, droit matériel en matière d'agression, traitement des preuves et introduction à la criminalistique) et des compétences beaucoup plus techniques et personnalisées (notamment les enquêtes sur les actifs virtuels, la criminalistique des logiciels malveillants et des données en temps réel, et les simulations de cyberattaques) grâce à des activités organisées en Ukraine et à l'étranger. Le projet a coopéré étroitement avec les institutions de formation des procureurs et des forces de l'ordre dans le cadre de sessions de formation spécialisées.

  L'une des contributions pratiques du projet en faveur de la justice pénale dans les affaires de crimes de guerre et de violations flagrantes des droits humains consiste à travailler avec les enquêteurs, les procureurs et le pouvoir judiciaire ukrainiens afin de mieux comprendre et appliquer les normes et possibilités internationales et nationales existantes. D'autres résultats du projet sont la finalisation du rapport sur les crimes de cyber agression et la préparation de la position nationale sur l'applicabilité du droit international humanitaire aux cyberattaques. Ces deux résultats ont été obtenus grâce à étroite collaboration avec les partenaires nationaux.

  Le projet a également poursuivi son travail avec la société civile et les médias (organisations de victimes, journalistes d'investigation et autres groupes concernés) en dispensant des cours de base sur la cybercriminalité, les preuves électroniques et le renseignement d'origine sources ouvertes. Des experts en cybersécurité, ainsi que des entités du secteur privé et des infrastructures critiques, ont été réunis pour suivre une formation et discuter des moyens d'assurer un meilleur accès et un meilleur échange d'informations et de preuves concernant les crimes de guerre et les violations flagrantes des droits humains.

  En 2025, le projet a touché près de 600 homologues ukrainiens grâce à 29 activités ciblant tous les domaines politiques du projet.

- Dans le cadre du projet **CyberSEE** sur le renforcement de la lutte contre la cybercriminalité et les preuves électroniques en Europe du Sud-Est et en Türkiye :

Des progrès significatifs ont été réalisés dans toute la région dans la mise en œuvre du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest). L'Albanie, le Monténégro, la Macédoine du Nord et la Serbie ont fait avancer les processus de réforme juridique grâce au soutien du projet, sous la forme de consultations de haut niveau, d'ateliers techniques, d'évaluations législatives et de recommandations de rédaction sur mesure.

En Bosnie-Herzégovine, les préoccupations institutionnelles initiales ont été prises en compte grâce à des actions de sensibilisation menées par des praticiens et soutenues par le projet, ce qui a abouti à la signature du Deuxième Protocole additionnel par le pays en novembre 2025.

La Türkiye a engagé des modifications de sa législation pénale afin d'introduire des dispositions modernes en matière de cybercriminalité et de preuves électroniques, avec le soutien du projet et des recommandations conformes aux normes de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

En Serbie, la stratégie de lutte contre la cybercriminalité (2026-2030) et son premier plan d'action (2026-2028) ont été finalisés en septembre 2025 avec le soutien de CyberSEE.

Les capacités des autorités de justice pénale ont été renforcées grâce à des programmes de formation structurés élaborés avec des institutions de formation nationales, comprenant des programmes d'études sur la cybercriminalité, des pools de formateurs nationaux, la formation de formateurs, des systèmes de certification et une formation progressive, du niveau de base au niveau avancé, pour la police et le pouvoir judiciaire. Les interventions pratiques se sont concentrées sur des domaines prioritaires tels que l'exploitation et les abus sexuels des enfants en ligne et l'utilisation illégale des cryptomonnaies. Des formats innovants, tels que les Cyber Games, se sont avérés efficaces pour améliorer les compétences opérationnelles et la coopération internationale.

Le projet a soutenu l'engagement des services répressifs dans les cadres européens et régionaux, notamment la plateforme pluridisciplinaire européenne contre les menaces criminelles (EMPACT), et a renforcé la coopération opérationnelle avec Europol, INTERPOL et Eurojust. Les capacités ont été encore renforcées en matière de coopération internationale, d'échange d'informations avec les institutions de cybersécurité et de collaboration avec le secteur privé grâce à des ateliers spécialisés, des modèles et des outils juridiques conformes au Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

La coopération interinstitutionnelle et entre les secteurs public et privé a été renforcée grâce à des réunions régionales, des formations conjointes, des exercices basés sur des cas concrets et des forums multipartites, notamment le Dialogue européen sur la gouvernance de l'internet (EuroDIG) et le Dialogue sur la gouvernance de l'internet en Europe du Sud-Est (SEEDIG).

Des événements majeurs tels que la Conférence sur l'économie souterraine et la Conférence CYBERVAW ont favorisé la coopération mondiale, les approches centrées sur les survivants et les réponses communes aux cybermenaces émergentes.

Le projet a soutenu 80 activités au cours de la période couverte par le rapport.

- Dans le cadre du projet **CyberSPEX** sur le renforcement de la coopération entre les États membres de l'UE en matière de preuves électroniques par le biais du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) :

  Le projet a aidé les États membres de l'UE à mettre en œuvre le Deuxième Protocole additionnel au niveau national grâce à des actions bilatérales et régionales coordonnées. Les principales parties prenantes de l'UE, notamment le Réseau judiciaire européen sur la cybercriminalité, le CEPOL et le projet SIRIUS, ont été associées afin de garantir la cohérence et la durabilité des activités futures.

  Les rédacteurs juridiques et les praticiens des 27 États membres de l'UE ont amélioré leur compréhension du Protocole et ont échangé leurs bonnes pratiques lors de réunions régionales couvrant les régions de la Baltique et de la Scandinavie, de l'Europe centrale et orientale, de la Méditerranée et de l'Europe occidentale. Ces réunions ont accéléré les processus nationaux de mise en œuvre, permettant ainsi des progrès significatifs en Autriche, en Estonie, en Hongrie, en Italie, en Lettonie, en Slovénie et en Suède. La Hongrie est devenue le premier État membre de l'UE à promulguer sa législation de mise en œuvre et de ratification en décembre 2025[13].

  Les 27 États membres de l'UE ont bénéficié d'un soutien sous la forme de documents de mise en œuvre complets, notamment un modèle d'évaluation juridique, un guide de mise en œuvre, un manuel sur l'interaction entre le Protocole et les instruments de l'UE, ainsi que des modèles de coopération au titre des articles 6 à 9 élaborés dans le cadre de CyberSPEX. Ces ressources sont désormais utilisées dans tous les projets du Bureau.

  Les praticiens de l'application de la loi ont été formés aux procédures de coopération internationale dans le cadre d'un séminaire dédié au sein du cours « Échange transfrontalier de preuves électroniques » du CEPOL, dispensé en coopération avec le Réseau européen de formation judiciaire. Les États membres ont également échangé leurs expériences avec d'autres parties lors d'ateliers et de conférences internationaux majeurs organisés avec des partenaires tels que EUROJUST, GLACY-e et CyberSEE.

  Des ateliers ciblés organisés dans les pays concernés ont apporté leur soutien aux groupes de travail provisoires en Finlande, en Slovénie et en République slovaque. CyberSPEX a en outre encouragé les États membres de l'UE non-signataires à adhérer au protocole, contribuant ainsi à la signature de la Lettonie en mars 2025. Un soutien supplémentaire a été apporté à l'Irlande, où une visite sur place a été menée en novembre 2025 par le Directeur général des droits humains et de l'État de droit du Conseil de l'Europe (DGI), accompagné du président du Comité de la Convention sur la cybercriminalité. Le projet est en dialogue avec ses homologues afin de soutenir le processus interne de modernisation de la loi sur l'interception en Irlande, dernière étape manquante pour la ratification de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

13. Voir également la note de bas de page n° 8.

Les États membres de l'UE ont acquis une meilleure compréhension de la coopération entre les secteurs public et privé dans le cadre des enquêtes et des procédures pénales lors d'un deuxième atelier organisé par le Comité de la Convention sur la cybercriminalité et CyberSPEX avec des prestataires de services et des représentants du secteur.

Au total, le projet a soutenu 47 activités au cours de la période considérée.

- Dans le cadre du projet **CyberSouth+** sur le renforcement de la coopération en matière de cybercriminalité et les preuves électroniques dans la région du voisinage méridional :

  L'accent a été mis davantage sur la consolidation du dialogue législatif, le renforcement des capacités spécialisées et la traduction de la coopération en résultats opérationnels en Algérie, en Égypte, en Jordanie, au Liban, en Libye, au Maroc, en Palestine*[14] et en Tunisie.

  Le dialogue législatif a progressé grâce à des échanges régionaux sur les normes internationales, notamment la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), la Convention des Nations Unies et le Premier Protocole additionnel à la Convention de Budapest. Le Maroc a progressé dans la modification de son code de procédure pénale, tandis que d'autres pays partenaires se sont engagés dans une réflexion législative préparatoire, notamment sur des domaines émergents tels que la cyberviolence et les implications de l'intelligence artificielle.

  La formation judiciaire a été renforcée grâce à des modules avancés, des échanges sur les manuels de formation nationaux et une évolution vers des approches modulaires. Cela a notamment consisté à adapter les méthodologies de formation judiciaire en Égypte et à mettre en œuvre des cours HELP et des formations judiciaires avancées dans plusieurs pays. Les capacités des services répressifs ont été renforcées grâce à des formations de plus en plus spécialisées et axées sur la pratique, notamment des cours basés sur des scénarios et des exercices régionaux. Les domaines prioritaires comprenaient l'exploitation et les abus sexuels des enfants en ligne, la cyberviolence à l'égard des femmes, la criminalité liée aux cryptomonnaies, les ransomwares et la criminalistique numérique avancée.

  La coopération opérationnelle est allée au-delà de la formation pour passer à la pratique, notamment grâce à des exercices régionaux de coopération en matière de cybercriminalité, à la participation aux Cyber Games et à des activités conjointes impliquant des acteurs chargés de l'application de la loi et de la cybersécurité, notamment la conférence régionale sur la gestion des crises en cas de cyberattaques et le lancement de la première opération régionale conjointe de lutte contre la cybercriminalité dans la région MENA dans le cadre d'INTERPOL. Ces efforts ont mis en évidence une solide expertise régionale, les praticiens de la région ayant obtenu des résultats remarquables lors d'exercices opérationnels compétitifs.

14. *Cette désignation ne doit pas être interprétée comme une reconnaissance de l'État de Palestine et ne préjuge pas des positions individuelles des États membres sur cette question.

La coordination avec les partenaires régionaux et internationaux, notamment INTERPOL, Europol, Eurojust, le DCAF et d'autres initiatives financées par l'UE, est restée au cœur de la mise en œuvre, tandis que la participation à des forums internationaux majeurs a favorisé les échanges interrégionaux et la visibilité de l'expérience régionale.

Le projet a soutenu 44 activités au cours de la période considérée.

- Dans le cadre du **Projet Octopus** qui soutient la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), de ses protocoles additionnels et des normes connexes à l'échelle mondiale :

  Le Projet Octopus sert de plateforme clé pour réunir les parties à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) lors des réunions du Comité de la Convention sur la cybercriminalité, permettant ainsi un dialogue politique coordonné et l'échange de bonnes pratiques en matière de lutte contre la cybercriminalité. En fournissant une assistance technique et un renforcement des capacités ciblé, le projet facilite l'adhésion de nouveaux pays à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), renforçant ainsi l'impact et la légitimité de la Convention à l'échelle mondiale. En outre, le projet soutient les travaux de fond du Comité de la Convention sur la cybercriminalité en promouvant des cadres législatifs harmonisés, une coopération transfrontalière efficace et des mécanismes durables pour la mise en œuvre des dispositions de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

  Des progrès significatifs ont été réalisés dans la promotion de réponses mondiales à la cybercriminalité et dans la promotion de l'utilisation efficace des preuves électroniques. Des réformes législatives ont été soutenues et mises en œuvre dans de nombreux pays, notamment aux Seychelles, au Kazakhstan, en Malaisie, au Bénin, en Sierra Leone, aux Fidji, au Pérou et en Zambie, favorisant une plus grande harmonisation avec la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et son deuxième protocole additionnel.

  Le projet a développé des ressources pratiques, telles qu'un manuel destiné à guider les réformes législatives en matière de cybercriminalité dans le Pacifique, et a fourni un soutien de niveau expert aux pays engagés dans la réforme des politiques et la mise en œuvre du Deuxième Protocole additionnel.

  En outre, les normes de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) ont été promues conjointement avec l'OSCE au Tadjikistan et au Kirghizistan, élargissant ainsi la portée internationale du projet.

  Le renforcement des capacités a été accéléré grâce à des formations ciblées dispensées à plus de 50 professionnels de la justice pénale et des forces de l'ordre de la Grenade, d'Antigua-et-Barbuda et de toute l'Asie du Sud-Est, axées sur les enquêtes et les poursuites en matière de cybercriminalité, le traitement des preuves électroniques et les domaines émergents tels que les ransomwares et les enquêtes cryptographiques.

  Le projet Octopus a également amélioré le partage des connaissances grâce à la maintenance et à l'utilisation élargie de la ressource Cyberviolence, de la plateforme Octopus et de la plateforme en ligne CYBOX, facilitant l'échange d'expertise et le développement de supports d'apprentissage en ligne pour la communauté mondiale de la justice pénale.

La participation à des événements majeurs, notamment la conférence Octopus, la conférence Europol sur la cybercriminalité et la réunion du réseau 24/7, a renforcé la coopération internationale, le partage des meilleures pratiques et le renforcement des capacités sur des thèmes prioritaires tels que l'intelligence artificielle, la cyberviolence et la cybercriminalité fondée sur le genre.

Dans l'ensemble, le projet Octopus a joué un rôle déterminant dans l'élaboration des politiques et des pratiques dans la lutte mondiale contre la cybercriminalité.

De nouvelles contributions volontaires ont été reçues en 2025 de la part de Malte, des Pays-Bas, du Royaume-Uni, du Canada et du Japon.

Grâce à l'action de **CYBERKOP**[15] du projet Octopus, les capacités des autorités de justice pénale ont été renforcées par l'élaboration et la mise en œuvre d'un programme de formation dédié à l'enquête sur les cybercrimes destiné aux premiers intervenants au sein de la police du Kosovo*[16], complété par une formation spécialisée en matière de renseignement d'origine sources ouvertes pour les enquêteurs et les procureurs, une formation de base sur la cybercriminalité et la participation à des programmes de certification des formateurs. Ces interventions ont contribué à harmoniser les pratiques d'enquête et à accroître le nombre de formateurs nationaux qualifiés.

Cette action a également contribué à améliorer le cadre juridique et judiciaire en participant à la rédaction de la loi sur la protection des données à caractère personnel pour les institutions chargées de l'application de la loi et en renforçant les capacités des magistrats à traiter la cybercriminalité et les preuves électroniques grâce à une formation judiciaire ciblée. La coopération judiciaire internationale a été encore renforcée grâce à une visite d'étude au Conseil de l'Europe, incluant la Cour européenne des droits de l'homme. L'atelier européen sur le traitement des dossiers a marqué une étape importante au niveau régional, démontrant un alignement renforcé sur les normes internationales, les garanties en matière de droits humains et le dialogue politique sur la protection des données.

Le projet a soutenu 65 activités au cours de la période considérée.

- Dans le cadre du projet **GLACY-e** sur le renforcement de l'action mondiale contre la cybercriminalité :

  En 2025, trois pays sélectionnés dans le cadre du projet (Sao Tomé-et-Principe, le Rwanda et Vanuatu) sont devenus parties à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest), tandis que les Fidji ont signé le deuxième protocole additionnel.

  Des réformes législatives sur la cybercriminalité ont été activement soutenues au Bénin, en République dominicaine, au Ghana, au Malawi, en Malaisie, au Mozambique, au Nigéria et en Uruguay, parallèlement à une aide à la réforme de la protection des données aux Fidji et au Mozambique.

  L'Argentine, le Kenya et le Malawi ont été intégrés au projet en tant que pays sélectionnés.

15. L'action CYBERKOP consiste en un ensemble d'activités menées dans le cadre du projet Octopus spécifiquement pour le Kosovo*.
16. *Toute référence au Kosovo, que ce soit à son territoire, à ses institutions ou à sa population, doit se comprendre en pleine conformité avec la Résolution 1244 du Conseil de sécurité des Nations Unies et sans préjuger du statut du Kosovo.

Les efforts de renforcement des capacités ont été globaux, 75 professionnels de 22 pays asiatiques ayant amélioré leur expertise en matière de réponse aux incidents cybernétiques grâce à l'opération « Secure », à laquelle le projet a contribué, et au renforcement des compétences des formateurs nationaux et à l'élargissement du vivier de formateurs nationaux au Brésil, en Colombie, en République dominicaine et au Ghana. L'intégration de modules de formation sur la cybercriminalité dans les académies judiciaires colombiennes a été soutenue, et plusieurs ateliers au Chili ont été consacrés à l'élaboration de modules de formation sur l'intelligence artificielle et la cybercriminalité.

Le projet a également contribué à la création de procédures opérationnelles standard aux Fidji et en Sierra Leone, renforçant ainsi leur capacité à répondre efficacement aux menaces de cybercriminalité. Il est important de noter que les points de contact 24/7 ont été améliorés au Bénin, en Côte d'Ivoire et au Cameroun, et qu'un manuel sur la mise en œuvre de la législation en matière de cybercriminalité a commencé à être élaboré lors de la première réunion en personne du sous-comité PILON, Réseau des responsables juridiques des îles du Pacifique.

Le projet a coorganisé avec succès la troisième édition du Forum africain sur la cybercriminalité et les preuves électroniques, accueilli par le gouvernement kenyan. L'événement a réuni plus de 350 participants de haut niveau, parmi lesquels des décideurs politiques, des professionnels de la justice pénale et des spécialistes de la cybersécurité de toute l'Afrique.

Grâce à des réunions régionales et à des formations ciblées, le projet a renforcé la collaboration et l'apprentissage entre les pays pivots, notamment lors d'événements phares tels que la conférence Octopus. Des exercices spécialisés ont amélioré la coopération en matière de cybercriminalité et de preuves électroniques entre les États insulaires du Pacifique, tandis que des formations en ligne avancées sur l'exploitation sexuelle des enfants ont favorisé l'apprentissage entre pairs parmi les pays GLACY-e et leurs partenaires d'Europe du Sud-Est et de Türkiye. Le projet a soutenu la septième opération annuelle du groupe de travail sur l'identification des victimes en Asie, la plus importante jamais organisée, permettant d'identifier et de hiérarchiser des affaires impliquant 136 enfants et 70 suspects à partir de plus de 33 000 images et vidéos, et facilitant ainsi des actions d'enquête dans plusieurs juridictions.

En outre, les pays pivots et d'autres pays sélectionnés ont bénéficié d'un soutien pour participer à plusieurs événements internationaux et régionaux : la Conférence internationale sur la lutte contre la cyberviolence à l'égard des femmes (CYBERVAW), la Conférence sur l'investigation numérique 2025, l'atelier coorganisé par Eurojust et le Conseil de l'Europe sur le Deuxième Protocole additionnel, la Conférence 2025 sur l'économie souterraine, la réunion annuelle du réseau des points de contact 24/7, ainsi que la conférence EUROPOL. Les réunions de suivi avec les représentants de huit pays pivots ont permis d'identifier d'autres besoins en matière de renforcement des capacités dans le domaine de la cybercriminalité aux niveaux régional et national.

Le projet a soutenu 89 activités au cours de la période considérée.

Initiatives de renforcement des capacités

Grâce à ses différents projets, le Bureau a lancé en 2025 de nombreuses initiatives à fort impact dans les domaines d'exploitation et les abus sexuels des enfants en ligne, de la cyberviolence, de l'intelligence artificielle et de l'ingérence électorale.

OCSEA, Exploitation et abus sexuels des enfants en ligne : une approche multirégionale a été adoptée pour renforcer les capacités de lutte contre l'exploitation des enfants en ligne. Les représentants des forces de l'ordre en Algérie, au Maroc et en Égypte ont reçu une formation spécifique sur les enquêtes relatives aux cas d'OCSEA, comprenant des ateliers avancés et l'intégration de méthodologies médico-légales spécialisées.

La « Formation avancée sur la cybercriminalité en matière d'enquêtes sur l'exploitation et les abus sexuels des enfants en ligne et le renseignement d'origine sources ouvertes pour les pays du Partenariat oriental » a encore renforcé le partage des connaissances et les compétences pratiques dans les États du Partenariat oriental.

Des plans visant à élargir les cours et manuels de formation judiciaire de base et avancée sur l'exploitation et les abus sexuels des enfants en ligne ont été élaborés pour les actions futures, afin de garantir un impact durable et évolutif.

Cyberviolence : le Bureau a priorisé la lutte contre la cyberviolence en y intégrant une dimension de genre. La Conférence internationale sur la lutte contre la cyberviolence à l'égard des femmes (CYBERVAW) a établi un suivi axé sur l'action et des avancées législatives.

Des ressources fondées sur des données probantes, telles que la Resource cyberviolence, et des activités régionales ciblées en Asie du Sud-Est et dans d'autres régions, ont été développées et diffusées. L'intégration des travaux entre les conventions de Budapest, de Lanzarote et d'Istanbul a favorisé une approche globale de la cybercriminalité fondée sur le genre.

Des webinaires thématiques, une étude prévue sur la diffusion non consensuelle d'images intimes et des collaborations avec des organisations de la société civile ont permis d'assurer un large engagement et la diffusion des connaissances.

Intelligence artificielle (IA) : Reconnaissant le rôle croissant de l'IA dans les activités criminelles, le Bureau a organisé des ateliers régionaux afin de renforcer l'utilisation de l'IA dans les enquêtes sur la cybercriminalité. Ces activités ciblaient les acteurs des forces de l'ordre et du système judiciaire, offrant une formation aux outils techniques basés sur l'IA et abordant les défis législatifs et opérationnels posés par l'évolution des menaces. La Conférence Octopus comprenait des sessions spécifiques sur l'impact de l'IA sur la cybercriminalité.

Ingérence électorale : en réponse à la menace d'ingérence numérique dans les processus démocratiques, des exercices techniques régionaux et nationaux, des formations spécialisées et des discussions politiques axées spécifiquement sur la cyber-ingérence électorale ont été organisés. Il s'agissait notamment d'exercices de simulation destinés aux forces de l'ordre et aux responsables électoraux ukrainiens.

L'activité Cyber Games, un format plus interactif de renforcement des capacités, s'est avérée très pertinente et efficace. Elle a réuni des praticiens de toutes les régions dans le cadre d'exercices réalistes en équipe qui ont permis de renforcer les compétences opérationnelles dans des domaines tels que les ransomwares, la criminalistique numérique et les enquêtes sur les cryptomonnaies, tout en renforçant la coopération et la confiance internationales.

Ensemble, ces initiatives ont mis en évidence une stratégie globale et à plusieurs niveaux pour lutter contre les menaces complexes dans le cyberespace, tout en renforçant la collaboration internationale, la réforme juridique et la formation opérationnelle.

Partenariats et synergies

Les partenariats et les synergies avec d'autres organisations sont une caractéristique essentielle du renforcement des capacités par le Bureau. Ils contribuent à intensifier les activités et à multiplier l'impact.

En 2025, le Bureau a coopéré étroitement avec un large éventail de partenaires internationaux et régionaux. Il s'agissait notamment de l'UE et de certaines agences de l'UE (Europol, Eurojust, CEPOL), d'INTERPOL, de l'OSCE, du PILON, du CARICOM, de l'OECO et de diverses entités des Nations unies, afin de renforcer l'alignement des politiques, la coopération opérationnelle et le renforcement des capacités en matière de cybercriminalité et de preuves électroniques.

Grâce à des conférences conjointes, des formations, des exercices opérationnels et des consultations multipartites, ces partenariats ont soutenu les réformes législatives, la mise en œuvre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et de ses protocoles additionnels, et ont amélioré les enquêtes transfrontalières. Ils ont couvert de nombreux domaines tels que les ransomwares, les cryptomonnaies, l'exploitation et les abus sexuels des enfants en ligne ainsi que la cyberviolence. En outre, la collaboration s'est concentrée sur l'alignement de la lutte contre la cybercriminalité sur les normes en matière de droits humains, d'État de droit, de démocratie, d'égalité de genre et des normes de gouvernance Internet. Un exemple en est le soutien apporté à la première réunion en personne du sous-comité PILON, qui s'est concentrée sur la rédaction d'un manuel sur la mise en œuvre de la législation en matière de cybercriminalité, réunissant des experts afin de faire progresser les orientations pratiques alignées sur la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

Le Bureau a reçu la délégation de l'Union européenne à la Barbade et des États des Caraïbes orientales, l'OECO et la CARICOM/CARIFORUM, ainsi que des représentants des institutions compétentes chargées des politiques en matière de cybercriminalité et de cybersécurité à la Barbade, en République dominicaine, à la Grenade, au Guyana, en Jamaïque, au Suriname et à Trinité-et-Tobago. La réunion avait pour objectif de fournir des informations sur les réponses efficaces à la cybercriminalité.

Le Bureau a renforcé sa coopération substantielle avec d'autres secteurs du Secrétariat du Conseil de l'Europe afin de garantir des réponses cohérentes, fondées sur les droits et intersectorielles à la cybercriminalité et sur les preuves électroniques.

Par exemple, il a collaboré avec les départements chargés de l'égalité de genre et de la prévention de la violence, notamment pour faire progresser les réponses à la cyberviolence et à la violence à l'égard des femmes facilitée par la technologie. Cela s'est fait par le biais de la conférence CYBERVAW, de la ressource Cyberviolence et de contributions à des discussions politiques centrées sur les survivants et fondées sur les droits.

La coopération avec les acteurs de la protection de l'enfance a permis de renforcer les capacités en matière d'exploitation et d'abus sexuels des enfants en ligne, en alignant les réponses à la cybercriminalité sur les normes de la Convention de Lanzarote.

Le Bureau a également coopéré avec les bureaux extérieurs du Conseil de l'Europe, en particulier en Afrique du Nord, dans les Balkans occidentaux et en Europe orientale, afin de mener des activités intégrées de renforcement des capacités et de renforcer l'appropriation régionale.

Une collaboration plus poussée avec les acteurs de l'éducation et de la formation a permis de soutenir des stratégies durables de formation dans les domaines judiciaire et répressif, notamment la mise à jour des cours HELP et l'intégration de modules sur la cybercriminalité dans les programmes nationaux.

Dans le domaine de la gouvernance Internet, les partenariats ont été renforcés grâce à une collaboration avec le Dialogue européen sur la gouvernance de l'internet (EuroDIG) et le Dialogue sur la gouvernance Internet en Europe du Sud-Est (SEEDIG), qui encouragent le dialogue multipartite, la coopération entre les secteurs public et privé et l'alignement des politiques numériques sur les valeurs démocratiques et les cadres de l'UE.

4. Conclusions et perspectives

Tout au long de l'année, le Bureau a continué à promouvoir les normes du Conseil de l'Europe en matière de cybercriminalité et a renforcé la reconnaissance de l'Organisation en tant que leader mondial dans ce domaine et en matière de preuves électroniques. Pour ce faire, il a traduit la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) et ses protocoles additionnels en orientations politiques faisant autorité, en réformes législatives et en mécanismes de coopération pratiques mis en œuvre dans le monde entier grâce à des partenariats multipartites fiables.

Le succès du Bureau est renforcé par sa capacité à réunir les gouvernements, les organisations internationales, l'industrie et la société civile dans des forums politiques fiables, tels que le Comité sur la cybercriminalité), la Conférence Octopus et les groupes de travail thématiques, où les nouveaux défis sont traduits en réponses politiques cohérentes, fondées sur les droits et viables sur le plan opérationnel dans toutes les régions.

Au cours des 11 dernières années, grâce à la mise en œuvre d'environ 2 700 activités, le Bureau a produit des résultats, des retombées et un impact important. Cela inclut un intérêt accru pour la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest)et l'adhésion à celle-ci[17], l'alignement de la législation nationale des États du monde entier sur ses normes[18] et le renforcement des capacités des praticiens de la justice pénale, ainsi que le soutien à la négociation et à la mise en œuvre ultérieure du Deuxième Protocole additionnel à la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

Les principaux facteurs de réussite :

- Les relations du Bureau au sein d'une triade dynamique composée : (a) d'un cadre législatif de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest); (b) des travaux du Comité de la Convention sur la cybercriminalité; et (c) des projets individuels de renforcement des capacités.

- Le Bureau est au service des pays et des parties prenantes de toutes les régions du monde.

17. En 2013, 53 États étaient parties (41), l'avaient signé (2) ou avaient été invités à y adhérer (10). À la fin de 2025, 97 États étaient parties (81), l'avaient signé (2) ou avaient été invités à y adhérer (14).
18. Par exemple, en 2013, 70 États avaient défini dans leur droit pénal des infractions similaires à celles prévues par la Convention sur la cybercriminalité ; seuls six d'entre eux étaient africains. À la fin de 2025, 134 États avaient atteint cet objectif, dont 34 États africains.

- La pertinence de son travail et sa réputation reposent sur la qualité et la rapidité du soutien apporté aux pays, qui ont un impact au niveau stratégique, politique et opérationnel.

- La capacité à s'adapter et à formuler un soutien sur mesure pour répondre à l'évolution des besoins, qui comprend les menaces posées par l'évolution de la technologie, la guerre d'agression de la Russie contre l'Ukraine, augmentation des attaques par ransomware, menaces à la liberté d'expression, cyberviolence, fraude en ligne, et autres cybermenaces émergentes.

Les priorités pour 2026 et au-delà :

- Maintien et renforcement de la triade dynamique de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) (avec ses protocoles additionnels), du Comité de la Convention sur la cybercriminalité et du Bureau.

- Collecte de fonds pour assurer la poursuite du Projet Octopus, qui est essentiel pour faire progresser la coopération mondiale, soutenir les nouvelles adhésions et renforcer l'efficacité opérationnelle de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest).

- Assurance que le Bureau continue d'opérer au niveau mondial et, par conséquent, la facilitation de la diffusion d'autres normes du Conseil de l'Europe au-delà de l'Europe, conformément à la déclaration de Reykjavík, par exemple dans les domaines de l'IA, de la protection des données ou de la protection des enfants.

- Développement des activités de renforcement des capacités dans les domaines suivants : (a) la protection des enfants en ligne et la diffusion non consentie d'images intimes ; (b) les actifs virtuels en relation avec la cybercriminalité et les preuves électroniques ; et (c) l'IA.

- Développement des partenariats et les synergies avec d'autres organisations afin d'accroître la portée et l'impact des projets et des activités.

- Promotion, mise en œuvre et ratification du Deuxième Protocole additionnel sur les preuves électroniques, étant donné que ce protocole est essentiel pour que le cadre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest) reste pertinent.

- Engagement constructif dans le cadre de la nouvelle Convention des Nations Unies contre la cybercriminalité, notamment en coopérant avec l'ONUDC afin de promouvoir l'alignement entre les deux conventions et de mettre fortement l'accent sur les conditions et les garanties.

- Développement de l'action du Bureau dans de nouvelles régions, en lançant de nouveaux projets et en mobilisant des ressources supplémentaires.

Fort de plus d'une décennie de réalisations et d'impact, le Bureau est bien placé pour consolider et étendre son rôle de moteur mondial du Conseil de l'Europe dans la traduction des normes relatives à la cybercriminalité en réponses efficaces et fondées sur les droits, garantissant ainsi la pertinence continue du cadre de la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest)et renforçant les droits humains, la démocratie et l'État de droit dans la lutte contre la cybercriminalité à l'échelle mondiale.

5. Table des abréviations

Abréviation	Nom complet
IA	Intelligence artificielle
CARICOM	Communauté des Caraïbes
CEPOL	Agence de l'Union européenne pour la formation des services répressifs
DCAF	Centre pour la gouvernance du secteur de la sécurité
ECTEG	Groupe européen pour la formation et l'éducation en matière de cybercriminalité
EMPACT	Plateforme pluridisciplinaire européenne contre les menaces criminelles
UE	Union européenne
EuroDIG	Dialogue européen sur la gouvernance de l'internet
Eurojust	Agence de l'Union européenne pour la coopération en matière de justice pénale
Europol	Agence de l'Union européenne pour la coopération des services répressifs
GFCE	Forum mondial de l'expertise cybernétique
INTERPOL	Organisation internationale de police criminelle
OAS	Organisation des Etats américains
OECS	Organisation des États des Caraïbes orientales
OSCE	Organisation pour la sécurité et la coopération en Europe
PILON	Réseau des responsables juridiques des îles du Pacifique
SEEDIG	Dialogue sur la gouvernance Internet en Europe du Sud-Est
T-CY	Comité de la Convention sur la cybercriminalité
UNCAC	Convention des Nations Unies contre la corruption
UNODC	Office des Nations Unies contre la drogue et le crime
UNTOC	Convention des Nations Unies contre la criminalité transnationale organisée
WB3C	Centre de Capacités Cyber des Balkans occidentaux