

N° 166
SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 27 novembre 2024

PROJET DE LOI

autorisant l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO),

PRÉSENTÉ

au nom de M. Michel BARNIER,

Premier ministre

Par M. Jean-Noël BARROT,

Ministre de l'Europe et des affaires étrangères

(Envoyé à la commission des affaires étrangères, de la défense et des forces armées, sous réserve de la constitution éventuelle d'une commission spéciale dans les conditions prévues par le Règlement.)

EXPOSÉ DES MOTIFS

Mesdames, Messieurs,

L'Accord entre le gouvernement de la République française, le Monténégro et la République de Slovénie a été signé le 16 octobre 2023 à Tirana (ci-après l'Accord) pour la partie française par Mme Laurence BOONE, Secrétaire d'État chargée de l'Europe, pour la partie monténégrine par M. Dristan ABAZOVIC, Président du gouvernement du Monténégro et, pour la partie slovène, par Mme Natasa PIRC MUSAR, Présidente de la République de Slovénie.

L'accord tend à créer un Centre de développement des capacités cyber dans les Balkans occidentaux (Albanie, Bosnie-Herzégovine, Kosovo, Macédoine du Nord, Monténégro, Serbie) en lui octroyant le statut d'organisation internationale (ci-après le C3BO). Le siège du centre est prévu au Monténégro, à Podgorica.

Cet accord signé par trois pays qualifiés de « fondateurs » a pour objet de renforcer la cyber-résilience⁽¹⁾ des Balkans par des activités de formation et de sensibilisation. Les objectifs du C3BO sont de renforcer les capacités opérationnelles des services de police et de justice, la prévention des attaques cyber et la gestion des risques.

Le C3BO vise à former des experts, au sein des agences, administrations, forces de police et de sécurité régionales. Il permettra d'approfondir la coopération entre tous les acteurs régionaux et d'harmoniser les normes applicables dans la perspective de leur adhésion future à l'Union européenne.

L'accord d'adhésion comprend un préambule avec sept considérants, huit parties et vingt-quatre articles.

⁽¹⁾ La cyber-résilience est la capacité d'une structure, d'un État à prévenir les incidents de cybersécurité, à y résister et à s'en relever. La cyber-résilience implique d'accepter que les violations soient inévitables et de choisir de se préparer à l'événement à l'avance. Elle suppose la mise en place de mesures de prévention, de détection et de réponse aux incidents, ainsi que la planification de la reprise après le sinistre et la continuité des activités.

Les considérants du préambule mentionnent le processus ayant conduit à la création du C3BO et à la nécessité de renforcer les capacités cyber pour les acteurs régionaux.

La partie I « CRÉATION » énonce le périmètre d'attribution du C3BO et les éléments constitutifs de son statut. Elle comprend quatre articles.

L'article 1^{er} « Définitions » s'attache à apporter dix définitions applicables à l'accord. Elles précisent notamment la qualité et le positionnement des membres qu'ils soient fondateurs ou non, appartenant ou non aux Balkans occidentaux ainsi que leur possibilité de faire partie des organes principaux du C3BO.

L'article 2 « Création et statut » définit le nom du Centre et lui accorde le statut du droit international.

L'article 3 « Siège » fixe le siège du C3BO au Monténégro, à Podgorica.

L'article 4 « Objectif et activités » rappelle l'objectif du Centre dans le cadre de ses activités de cybersécurité de lutte contre la cybercriminalité ainsi que son rôle dans le domaine de la coopération internationale et du cyberspace.

La partie II « MEMBRES du C3BO » comprend quatre articles. Elle définit la qualité des différents membres, leur condition de participation au Conseil d'administration et leurs obligations financières.

Les articles 5 « Membres fondateurs », 6 « Autres membres appartenant au groupe des six pays des Balkans occidentaux » et 7 « Autres membres », rappellent la liste des membres fondateurs et la possibilité d'adhérer des pays faisant partie des Balkans occidentaux. Ils indiquent également les conditions d'adhésion, par le vote du Conseil d'administration, des pays tiers ou des organisations internationales. Ces articles fixent également la composition du Conseil d'administration et ses attributions en matière d'élargissement à de nouveaux membres. Ils indiquent également les obligations de chacun en matière de contribution financière.

L'article 8 « Suspension » précise les modalités et les conditions de suspension d'un membre ou de son droit de vote.

La partie III « GOUVERNANCE ET ORGANISATION » comprend quatre articles. Elle décrit les organes principaux du C3BO, rappelle leur composition et leur attribution ainsi que la possibilité de création d'autres organes subsidiaires qui pourraient s'avérer nécessaires au fonctionnement.

Les articles 9 « Structure du C3BO », 10 « Conseil d'administration », 11 « Conseil consultatif » et 12 « Secrétariat » précisent pour chacun de ses organes principaux leur composition, organisation et fonctionnement. L'article 12 détermine le mode de nomination et les attributions du directeur général en tant que représentant légal du C3BO.

La partie IV « FINANCEMENT » comprend un article unique.

L'article 13 « Ressources financières et responsabilité » définit les responsabilités de ses membres et permet autant des contributions en nature que financières. Il évoque également la possibilité des participations par des partenaires ou des bailleurs de fonds.

La partie V « RÈGLEMENT INTÉRIEUR ET AUTRES RÈGLEMENTS INTERNES » comprend un article unique, l'article 14 ayant le même titre que cette partie. Il fixe les conditions d'adoption de ces règlements.

La partie VI « TRAITEMENT DES DONNEES ET HABILITATION DE SECURITE » comprend deux articles.

L'article 15 « Traitement des données » renvoie au règlement intérieur l'adoption des règles relatives à la protection des données afin d'être en conformité avec les obligations internationales et le cas échéant européennes.

L'article 16 « Habilitation de sécurité » indique la procédure applicable aux candidats pour être habilités.

La partie VII « DISPOSITIONS FINALES » comprend huit articles.

Les articles 17 « Réserve », 18 « Signatures, ratification, approbation et adhésion », 19 « Entrée en vigueur », 20 « Amendements », 21 « Retrait », 22 « Dénonciations », 23 « Règlement des différends », 24 « Dépositaires » déterminent les modalités d'entrée en vigueur, d'amendement et de dénonciation de l'accord. Ils rappellent les conditions d'adhésion ou de retrait des membres ainsi que les modalités de règlement des différends. Le dépositaire de l'accord est le Monténégro.

Telles sont les principales observations qu'appelle l'Accord entre le Gouvernement de la République française, le Monténégro et la République

de Slovénie signé le 16 octobre 2023 à Tirana portant création d'un Centre de développement des capacités cyber dans les Balkans occidentaux en tant qu'organisation internationale.

DÉCRET DE PRÉSENTATION

Le Premier ministre,

Sur le rapport du ministre de l'Europe et des affaires étrangères,

Vu l'article 39 de la Constitution,

Décète :

Le présent projet de loi autorisant l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO), délibéré en conseil des ministres après avis du Conseil d'État, sera présenté au Sénat par le ministre de l'Europe et des affaires étrangères, qui sera chargé d'en exposer les motifs et d'en soutenir la discussion.

Fait à Paris, le 27 novembre 2024

Signé : Michel BARNIER

Par le Premier ministre :

Le ministre de l'Europe et des affaires étrangères

Signé : Jean-Noël BARROT

**Projet de loi autorisant l'approbation de l'accord portant création du
Centre de développement des capacités cyber dans les Balkans
occidentaux (C3BO)**

Article unique

Est autorisée l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO), fait à Tirana le 16 octobre 2023, et dont le texte est annexé à la présente loi.

RÉPUBLIQUE FRANÇAISE

Ministère de l'Europe
et des affaires étrangères

**TEXTE SOUMIS À LA DÉLIBÉRATION
DU CONSEIL DES MINISTRES**

**Projet de loi
autorisant l'approbation de l'accord portant création du Centre de développement
des capacités cyber dans les Balkans occidentaux (C3BO)**

NOR : EAEJ2422845L/Bleue-1

ÉTUDE D'IMPACT

I. Situation de référence

La forte croissance des usages numériques depuis la fin du XX^e siècle a contribué au développement des opportunités offertes par le cyberspace¹ et, en parallèle, à l'apparition de nouvelles menaces. L'extension continue de cet espace et donc des surfaces d'attaque, la dépendance accrue des sociétés à son fonctionnement et l'interdépendance numérique des Etats donnent des capacités de nuisance nouvelles aux acteurs malveillants, qu'ils soient étatiques ou non-étatiques. Ces nouveaux modes d'action sont employés tantôt par des acteurs à visée criminelle, tantôt utilisés par des Etats à des fins d'espionnage, de déstabilisation ou d'agression ou comme instrument d'ingérence.

Aujourd'hui les lacunes dans la sécurisation des réseaux d'un Etat peuvent constituer une source de vulnérabilités au niveau international. La multiplication des attaques par *supply chain* (attaque par les chaînes d'approvisionnement numériques) illustre la fragilité de l'espace numérique dans lequel le niveau de sécurité des réseaux informatiques est défini par le maillon le plus faible de la chaîne du réseau. En contribuant au renforcement des capacités d'un Etat tiers sur le long terme, un Etat peut espérer bénéficier d'un retour de ce soutien (lutte contre la cybercriminalité, échange d'informations, rapprochement des modèles de gouvernance, relations bilatérales renforcées...).

¹ Espace constitué par les infrastructures connectées relevant des technologies de l'information, notamment et internet.

Dans ce contexte, les Nations Unies ont reconnu à de multiples reprises que le renforcement capacitaire constituait un élément central des efforts visant à élaborer et mettre en œuvre le cadre normatif de comportement responsable des Etats dans le cyberspace². Ainsi, le rapport final du Groupe d'experts gouvernementaux 2019-2021 (A/76/135, §87) souligne que *« l'intensification de la coopération, conjuguée à une assistance plus efficace et à un renforcement des capacités en matière de sécurité numérique associant d'autres parties prenantes, [...] peut aider les États à appliquer le cadre de promotion d'un comportement responsable concernant l'utilisation qu'ils font des technologies numériques. Ces efforts accrus sont essentiels pour combler les fossés qui existent au sein des États et entre eux sur les questions politiques, juridiques et techniques touchant à la sécurité numérique. »* En effet, le déficit de mise en œuvre du cadre de comportement responsable des Etats dans le cyberspace n'est pas seulement lié à une absence de volonté politique mais, bien souvent, à une insuffisante appropriation de ce cadre normatif en raison des disparités de moyens et de capacités techniques ou institutionnelles entre pays.

Ainsi, en parallèle des efforts conduits pour assurer la cyberdéfense de la nation (organisation de la cyberdéfense, protection des activités sensibles, lutte contre la cybercriminalité, coopération et régulation internationale) et garantir la cybersécurité de la société (régulation politique, industrielle de cybersécurité, formation à la cybersécurité), la France contribue au renforcement de la cyberrésilience³ de ses partenaires européens et internationaux. Dans un espace de conflictualité en partie immatériel où les attaquants se jouent des frontières, le renforcement de notre résilience nationale doit s'accompagner d'un effort de renforcement des capacités au niveau global, tel que le soulignait déjà la Revue stratégique de cyberdéfense de la France de février 2018⁴ en précisant que *« nos coopérations structurelles, techniques et opérationnelles [...] sont des instruments stratégiques concourant de manière directe et indirecte à consolider notre sécurité nationale et notre influence. [Elles sont] un vecteur efficace pour promouvoir l'offre et l'expertise françaises en matière de cybersécurité »*. Le 9 novembre 2022, la Revue nationale stratégique a réaffirmé que *« la résilience de la France dépend [...] de celle de ses partenaires européens et internationaux ainsi que de la sécurité et de la stabilité du cyberspace dans son ensemble. »*

Les activités de coopération structurelle, ou de renforcement capacitaire, en matière cyber, recouvrent un champ nouveau de coopération et sont développées dans les régions stratégiques pour la politique étrangère française. Le renforcement capacitaire cyber est entendu comme la conduite d'actions de coopération permettant le transfert de connaissances et de compétences, voire de technologies, visant à renforcer la doctrine, les modèles d'organisation ainsi que les capacités d'un partenaire étatique international, afin qu'il soit davantage en mesure d'assurer lui-même sa cybersécurité et puisse remplir ses obligations internationales en la matière. Dans ses efforts, la France veille à répondre à un besoin précis exprimé par les Etats, et à intégrer les points de vigilance adaptés à la situation de chacun d'entre eux.

¹ Voir par exemple le 2^e rapport annuel de progrès de l'OEWG 2021-2025 (A/78/265).

² La cyber-résilience est la capacité d'une structure, d'un Etat à prévenir les incidents de cybersécurité, à y résister et à s'en relever. La cyber-résilience implique d'accepter que les violations sont inévitables et de choisir de se préparer à l'événement à l'avance. Elle suppose la mise en place de mesures de prévention, de détection et de réponse aux incidents, ainsi que la planification de la reprise après le sinistre et la continuité des activités.

³ Revue stratégique de cyberdéfense de la France de février 2018.

Le voisinage oriental de l'Union européenne, en particulier les Balkans occidentaux (Albanie, Bosnie-Herzégovine, Kosovo, Macédoine du Nord, Monténégro, Serbie) est dans ce contexte une priorité française, notamment dans le cadre de la Communauté politique européenne et de l'intégration européenne. Les Etats de la région font par ailleurs face à une menace cyber s'étant récemment matérialisée par des attaques d'ampleur, avec des conséquences potentielles sur notre sécurité nationale.

A titre d'exemple, l'Albanie⁵ et le Monténégro ont été victimes de cyber attaques d'ampleur en 2022 et Podgorica a adressé une demande aux partenaires internationaux pour recevoir un soutien en prévention de futures attaques potentielles. L'Albanie et le Monténégro ont ainsi reçu l'appui des Etats-Unis, du Royaume-Uni et de la France. La guerre d'agression de la Russie contre l'Ukraine a par ailleurs des conséquences dans le cyberspace. L'ENISA⁶ a documenté des cyber opérations conduites par des acteurs parrainés par l'Etat russe contre des entités et des organisations en Ukraine et dans les pays qui soutiennent l'Ukraine. L'Union européenne a par ailleurs attribué publiquement à la Russie deux cyberattaques ayant eu des effets sur les intérêts européens, en 2022 s'agissant de la cyberattaque contre le satellite KA-SAT et en mai 2024⁷ à la suite de cyberattaques ayant visé des objectifs politiques en particulier en Allemagne et en République tchèque.

Le projet de Centre de développement de capacités cyber dans les Balkans occidentaux (C3BO) s'inscrit pleinement dans la stratégie interministérielle pour les Balkans occidentaux décidée en 2019 par le Président de la République⁸ et qui fait du développement du C3BO un des axes majeurs du pilier « sécurité » de notre stratégie de réengagement dans la région. Le projet doit permettre de remplir un double objectif. D'une part, un retour optimal en termes de sécurité intérieure pour la France et l'Union européenne en contribuant au renforcement d'un maillon faible et en permettant aux acteurs des Balkans occidentaux de traiter les problèmes liés à la cybercriminalité par eux-mêmes. D'autre part, une amélioration sensible de la coopération régionale dans les Balkans occidentaux et l'approfondissement des liens entre les pays de la région et l'Union européenne, dans la perspective de l'adhésion des six pays des Balkans occidentaux à l'UE.

Ce projet devra également composer avec un contexte régional très vulnérable aux activités de désinformation menées depuis l'étranger, qui se sont intensifiées ces dernières années. La Bosnie-Herzégovine, le Monténégro et la Serbie sont les pays les plus touchés par ces opérations russes d'information visant à décrédibiliser l'UE et l'OTAN dans la région.

⁵ Rupture des relations entre l'Albanie et l'Iran après une cyberattaque.

⁶ Site de l'Agence de l'Union européenne pour la cybersécurité.

⁷ Cyber opérations russes contre l'Ukraine : déclaration du haut représentant au nom de l'Union européenne.

⁸ Stratégie interministérielle pour les Balkans occidentaux, 2019.

II. Contexte historique et politique de la participation française

Pour faire face à ces défis cyber significatifs, tels que le cyberespionnage ou le cybersabotage, ou encore la mise en place d'agences nationales de sécurité, la France et la Slovénie ont choisi une approche en « Equipe Europe »⁹ pour co-construire un projet de renforcement des capacités et des compétences en matière de cybersécurité, de lutte contre la cybercriminalité et de cyberdiplomatie. Le Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO), basé à Podgorica (Monténégro), vise ainsi à améliorer le partage des bonnes pratiques et des politiques publiques et à renforcer les écosystèmes cyber des pays de la région, dans une perspective d'alignement avec l'acquis communautaire en matière de cybersécurité.

Depuis l'adoption de la directive NIS (*Network and Information System Security*) en 2016¹⁰, l'Union européenne s'est dotée d'un cadre réglementaire robuste pour assurer la cybersécurité des systèmes d'information, notamment au sein des infrastructures critiques. Pour les pays candidats à l'accession à l'Union européenne, la conformité à cet acquis communautaire présente un intérêt important.

A l'échelle de l'OTAN, les Alliés se sont également engagés à renforcer la protection de leurs systèmes d'information critiques, notamment par le *Cyber Defense Pledge* de 2016¹¹, dans un contexte stratégique où le cyberspace est devenu un champ de conflictualité à part entière. Les alliés des Balkans occidentaux ont pleinement un rôle à jouer dans le renforcement de la résilience cyber de l'espace euro-atlantique.

Par l'établissement du C3BO, la France, le Monténégro et la Slovénie renforcent leur partenariat politique au service de la sécurité.

A l'issue d'une mission de préfiguration conduite de janvier à avril 2022, et de rencontres avec différents experts de la région des Balkans occidentaux, la France et la Slovénie ont décidé conjointement de lancer un projet visant à l'établissement d'un centre dédié aux enjeux cyber. Il est apparu dès cette première étape que les États de la région étaient inégalement munis d'instruments tant techniques, politiques que juridiques visant à se prémunir contre les menaces cyber, laissant apparaître un besoin de structuration de la gouvernance de ces enjeux. Ainsi, à l'issue des nombreux entretiens réalisés, la mission de préfiguration a fait le constat d'un niveau d'expertise humaine et technique, certes existant, mais fortement variable d'un État à l'autre, les experts restant majoritairement attirés par le secteur privé, créant ainsi pour les administrations un manque en ressources humaines qualifiées. Parallèlement, dès les discussions entamées pour la création du Centre et dans ce contexte de manque de capacités cyber, les États ont exprimé leur souhait de renforcer la coopération internationale, notamment pour faciliter le partage d'informations et de bonnes pratiques à mettre en œuvre.

⁹ L'approche Team Europe adoptée par l'UE et ses Etats membres en 2020 est un engagement à produire un impact plus important et de meilleure qualité en mettant en place une coopération européenne au développement conjointe, coordonnée et plus efficace.

¹⁰ Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

¹¹ Organisation du Traité de l'Atlantique Nord (OTAN), Cyber Defence Pledge du 8 juillet 2016.

L'appropriation du projet est le premier pas vers sa pérennisation. En impliquant les parties prenantes dans tout le processus du projet, la France et la Slovénie se sont assurées que les initiatives sont mieux adaptées aux besoins locaux et peuvent être gérées efficacement à long terme. C'est pourquoi le Centre devait être implanté dans l'un des six pays de la région.

Tous les pays bénéficiaires du projet ont formulé une proposition d'hébergement du Centre régional. S'agissant du choix du pays hôte, prenant en compte tant les besoins techniques, pédagogiques et logistiques que les considérations politiques, la France et son partenaire slovène ont arrêté leur choix sur le Monténégro, pays membre de l'OTAN et candidat le plus avancé dans le processus d'intégration européenne¹², pour y implanter le C3BO. Le Monténégro, à l'issue d'un appel à candidatures, s'était montré le plus motivé des pays de la région et le seul à présenter une offre complète et cohérente. Pour l'heure le projet est financé très majoritairement par la France avec une participation de la Slovénie et une contribution du Monténégro. Cette contribution consiste en la mise à disposition de locaux pour l'implantation du C3BO.

III. Historique des négociations de l'accord

Une lettre d'intention tripartite a été signée entre la France, le Monténégro et la Slovénie le 16 novembre 2022, à Podgorica. Cet engagement de nature politique a fixé les grandes orientations de cette coopération cyber. Il prédéfinit notamment les organes de gouvernance et prévoit la création d'une organisation internationale, dotée d'une personnalité juridique propre. Il a été prévu que d'autres partenaires puissent également rejoindre cette organisation en qualité de membres, de contributeurs ou de partenaires.

Le 16 octobre 2023, à Tirana, dans le cadre du Sommet du Processus de Berlin,¹³ la France, le Monténégro et la Slovénie ont signé l'accord permettant l'octroi du statut d'organisation internationale au C3BO. Ce statut a pour objet d'intégrer au Centre les six pays des Balkans occidentaux (Albanie, Bosnie-Herzégovine, Kosovo, Macédoine du Nord, Monténégro, Serbie). Ils pourront devenir, dès l'entrée en vigueur de cet accord, membres de droit de cette structure par simple adhésion. Chaque membre appartenant au groupe des pays des Balkans occidentaux disposera de représentants au sein du Conseil d'administration et au conseil consultatif.

Après approbation et entrée en vigueur de l'accord, il est prévu d'élargir le Centre à de nouveaux membres, en priorité notamment les Etats membres de l'Union européenne, dans une logique de renforcement de la coopération et de l'intégration régionale. La sélection des nouveaux membres se fera par le biais de critères de compétence technique permettant de trouver des synergies, des axes de complémentarité avec d'autres projets. Les aspects politiques seront également pris en considération.

Dans cette perspective, ces nouvelles adhésions contribueront par ailleurs au financement des activités de formation.

¹² Le Monténégro a ouvert l'ensemble des 33 chapitres de négociations et en a clos provisoirement 3. Porté par une dynamique de réformes depuis novembre 2023, il pourrait clore 10 nouveaux chapitres d'ici la fin de l'année 2024.

¹³ Le Processus de Berlin est une initiative diplomatique lancée par l'Allemagne lors de la conférence des États des Balkans occidentaux, qui s'est tenue à Berlin en 2014 en vue d'accélérer les processus d'adhésion dans l'Union européenne des pays de la région.

IV. Présentation de la future organisation internationale C3BO

Le C3BO est unique tant dans sa forme que dans ses objectifs. Conjointement avec le partenaire slovène, le ministère de l'Europe et des Affaires étrangères a décidé de faire de ce centre une organisation internationale dans la perspective, notamment, de mettre en place une gouvernance inclusive intégrant les pays de la région, de maîtriser les finances du Centre, d'attirer des bailleurs internationaux autour d'un hub régional unique. Le statut d'organisation internationale sera apposé au C3BO, structure de dimension internationale dédiée à la formation à la cybersécurité, à la lutte contre la cybercriminalité et à la cyberdiplomatie. Ses locaux sont installés de façon permanente dans le Parc des Sciences et de la Technologie de Podgorica, au Monténégro.

Le fait d'être une organisation internationale implique plusieurs conséquences juridiques. Ce statut permet en effet d'octroyer une personnalité juridique internationale au C3BO. La Cour internationale de Justice note à cet égard que « [l]’organisation internationale est un sujet de droit international lié en tant que tel par toutes les obligations que lui imposent les règles générales du droit international, son acte constitutif ou les accords internationaux auxquels il est partie »¹⁴.

Les compétences de l'organisation sont définies par son acte constitutif, auquel l'organisation est tenue de se conformer¹⁵. Contrairement aux Etats, les compétences des organisations internationales sont strictement limitées à ce que les Etats ont décidé de lui déléguer.

Enfin, il peut être rappelé que l'expression « organisation internationale » renvoie généralement aux organisations inter-gouvernementales et non aux organisations non-gouvernementales¹⁶. Ainsi, même si divers acteurs (non-gouvernementaux ou privés) peuvent collaborer avec le C3BO, ce constat n'est pas de nature à remettre en question sa nature d'organisation internationale intergouvernementale.

L'objectif principal dans l'octroi du statut d'organisation internationale au Centre régional est d'associer les six pays des Balkans occidentaux, mais aussi, à terme, d'autres Etats membres de l'UE, à sa gouvernance. Dans cette perspective, les experts - issus de la région ou d'autres nationalités mais évoluant dans des projets développés dans les Balkans occidentaux - ont vocation à participer à la conduite des formations aux côtés des experts français et slovènes. Cette démarche est conduite dans un esprit de rapprochement avec l'Union européenne, en renforçant la coopération avec les Etats membres.

¹⁴ *Interprétation de l'Accord du 25 mars 1951 entre l'OMS et l'Égypte, Avis consultatif du 20 décembre 1980, 1980 Rep. C.I.J. 73, 89-90, para. 37.*

¹⁵ V. *Licéité de l'utilisation des armes nucléaires par un État dans un conflit armé, Avis consultatif du 8 juillet 1996, 1996 C.I.J. 66, 78-79, para. 25* (« La Cour a à peine besoin de rappeler que les organisations internationales sont des sujets de droit international qui ne jouissent pas, à l'instar des Etats, de compétences générales. Les organisations internationales sont régies par le ((principe de spécialité)), c'est-à-dire dotées par les Etats qui les créent de compétences d'attribution dont les limites sont fonction des intérêts communs que ceux-ci leur donnent pour mission de promouvoir. »).

¹⁶ Convention de Vienne sur le droit des traités, Art. 2 ; v. *Projet d'articles sur le droit des traités et commentaires, Art. 2, commentaire 14* (la Commission de droit international indique que « L'expression « organisation internationale » est définie ici comme s'entendant d'une organisation intergouvernementale, ce qui précise que les règles des organisations non gouvernementales n'entrent pas en ligne de compte »).

Comme énoncé ci-dessus, la forme juridique d'organisation internationale permettra d'associer à sa gouvernance un grand nombre d'acteurs intervenant dans la région, de façon à mutualiser les expertises et les moyens déployés. En effet, le C3BO a déjà été sollicité par de nombreuses institutions internationales, européennes, et des Etats membres, afin de nouer des partenariats, témoignant du rayonnement et de l'intérêt suscité.

L'organisation actuelle du centre s'articule, d'ici la ratification de l'accord, autour de cinq groupes de travail (juridique, finances, formations, infrastructures, coopération internationale) travaillant sous la supervision d'un comité de pilotage paritaire (France, Monténégro, Slovénie). Un directeur des études et deux formateurs issus de la police et de la gendarmerie françaises complètent à ce jour le dispositif. Enfin, un réseau de coordinateurs nationaux, issus des six pays des Balkans occidentaux, est régulièrement consulté pour faire remonter les besoins et acter les orientations du projet.

La première action de formation du C3BO s'est déroulée à Podgorica, dans les locaux de l'Université du Monténégro, du 8 au 12 mai 2023. Au total, en 2023, cinq formations se sont tenues au C3BO au profit des académies de police, des magistrats et des responsables de la sécurité des systèmes d'information (RSSI) de la région. Par ailleurs, un événement de sensibilisation a été organisé au profit de responsables politiques aux questions cyber.

Adaptés à chaque public, les cours sont partagés entre théorie et exercices pratiques. Une évaluation est réalisée à la fin de chaque session. Pour l'heure ces formations donnent lieu à des attestations de stage. A terme certaines seront diplômantes en partenariat avec des universités.

Pour l'année 2024, douze formations ont été programmées.

V. Objectifs de l'accord

Conformément à son article 4, « *l'objectif du C3BO est de renforcer la cyberrésilience des Balkans occidentaux grâce à la promotion d'une culture du cyberspace par la formation et la sensibilisation, à l'approfondissement des connaissances des praticiens et à la création d'un réseau régional de coopération* ».

Les activités développées en matière de lutte contre la cybercriminalité, de cybersécurité et de cyberdiplomatie s'articulent autour de trois axes :

1 – Diffusion d'une culture cyber par l'éducation et la sensibilisation

- Soutenir, susciter ou alimenter les actions de prévention, d'éducation et de sensibilisation à destination des publics touchés par la cybercriminalité ou acteurs dans la lutte contre la cybercriminalité, la cybersécurité ou la cyber hygiène¹⁷ ;
- Développer des actions de formation pour les services d'investigation et la justice mais également l'administration publique ;

¹⁷ La cyber hygiène désigne les pratiques et procédures utilisées pour maintenir la santé et la résilience de la sécurité des systèmes, appareils, réseaux et données, par exemple : **mots de passe forts et uniques, maintenance des logiciels et des systèmes, sauvegarde des données, sécurisation des réseaux Wi-Fi, formation des utilisateurs, chiffrement des données sensibles.**

- Créer des instruments dédiés à la formation des praticiens : construire, entretenir et animer un vivier de formateurs ;
- Élaborer un *curriculum* de formations « cybersécurité » dans les universités de la région : aborder ses enjeux, les étapes de son élaboration, la gestion de ses différentes composantes, ainsi que la dimension pratique qui lui est associée.

2 – Renforcement des capacités des professionnels de la cybersécurité (investigations, poursuites, prévention des attaques, gestion des risques)

- Identifier et cibler les professionnels appelés à monter en compétence pour pallier la pénurie de main d'œuvre qualifiée dans l'administration publique ;
- Renforcer et compléter le dispositif opérationnel : référents cyber Police et Justice, méthodologie de veille des systèmes d'information, de gestion d'incidents et d'évaluation du risque ;
- Développer l'expertise opérationnelle (investigation spécialisée et financière notamment).

3 – Renforcement de la coopération régionale et internationale

- Impliquer les décideurs clés, dont les directeurs d'agence et les diplomates, dans les enjeux de cyberdiplomatie ;
- Promouvoir la coopération régionale : capitaliser et partager les bonnes pratiques ;
- Faciliter l'échange d'expérience et encourager la coopération opérationnelle à l'échelle régionale.

VI. Conséquences estimées de la mise en œuvre de l'accord

Le présent accord emporte, à des degrés divers, des conséquences économiques (*a.*) ; environnementales (*b.*) ; juridiques (*c.*) ; sociales (*d.*) et financières (*e.*). Il a également des répercussions sur l'égalité femmes-hommes (*f.*) et vis-à-vis de la jeunesse (*g.*).

a. Conséquences économiques

L'implantation du Centre emportera tout d'abord des conséquences sur la qualification de la main d'œuvre dans les Balkans occidentaux, d'abord dans les administrations publiques, puis indirectement dans le secteur privé des pays de la région.

Ensuite, dans la mesure où le Centre doit encourager et accompagner les pays de la région dans le renforcement de la protection de leurs infrastructures, les entreprises spécialisées en cybersécurité et en lutte contre la cybercriminalité bénéficieront d'une commande publique qui devrait croître, notamment pour l'achat de logiciels et le renforcement capacitaire des structures publiques. Ces nouveaux débouchés présentent des opportunités pour le rayonnement de l'expertise française, y compris privée, à l'étranger.

Le C3BO engendrera de nombreuses missions d'expertise qui seront menées, notamment, par des professionnels d'entreprises françaises spécialisées sur des segments de niche du marché de la cybersécurité (*cyber threat intelligence, endpoint detection and response, gestion de la surface d'attaque*¹⁸, etc...). L'emploi de ressources du privé au profit des projets cyber doit permettre la valorisation de l'excellence des savoir-faire français ainsi que l'obtention de marchés locaux.

Le secteur privé peut ainsi constituer un partenaire clé dans la conduite des programmes du C3BO.

Une implication croissante des entreprises dans ces actions présente pour elles un intérêt certain :

- Accès à de nouveaux marchés, notamment dans le domaine de la formation, du conseil et de l'intégration en cybersécurité ;
- Valorisation de l'expertise de la filière française de cybersécurité et création de liens de confiance conférant à nos entreprises un positionnement stratégique dans la structuration d'écosystèmes locaux ;
- Renforcement du niveau général de cybersécurité visant à favoriser le développement de l'économie numérique dans son ensemble.

De manière générale, la mise en œuvre de l'accord aura pour conséquence de rehausser le niveau de compétences des agents publics de la région ayant des fonctions dans les domaines cyber, de valoriser l'emploi de jeunes talents, d'instaurer les allers-retours entre les sphères publique et privée et promouvoir les métiers cyber auprès des femmes de la région. Cet effort global de renforcement capacitaire cyber doit permettre d'atteindre un niveau de cyber-résilience permettant d'éviter ou de limiter les impacts des menaces cyber dans le fonctionnement régulier des pouvoirs et services publics.

b. Conséquences environnementales

Les activités du C3BO emporteront des conséquences environnementales en rapport principalement avec la consommation énergétique des bâtiments (serveurs, plateau technique etc.) et le transport des stagiaires et des formateurs.

¹⁸ La *Cyber Threat Intelligence (CTI)* définit la recherche, l'analyse et la modélisation de la menace cyber. Cela sert à prévenir et à détecter des attaques informatiques, de connaître préalablement la menace pour l'anticiper, c'est-à-dire prendre des contre-mesures défensives en amont et la détecter en temps réel si nécessaire. L'*Endpoint detection and response (EDR)* est un logiciel de détection des menaces de sécurité informatique sur les équipements numériques. Les EDR sont une évolution de l'antivirus et du pare-feu, particulièrement préconisés pour protéger les machines (ordinateurs, smartphone) et les serveurs. La gestion de la surface d'attaque (*Attack Surface Management - ASM*) est le processus d'identification, d'analyse et de gestion des différents points d'entrée que les attaquants (cybercriminels) pourraient exploiter pour obtenir un accès non autorisé au réseau d'une organisation. Cette gestion est un élément essentiel de la gestion des risques cyber car elle aide les acteurs à identifier les faiblesses de manière proactive et à y remédier avant qu'elles puissent être exploitées.

Le C3BO doit toutefois permettre d'accroître la capacité de cyberrésilience de la région, encourageant ainsi la promotion et l'emploi de solutions techniques afin de renforcer la sécurisation des installations critiques (type usine de production électrique...). Ces solutions sont de nature à réduire le risque d'un impact environnemental grave en cas de cyberattaques sur ces infrastructures.

c. Conséquences juridiques

Le Centre de développement des Capacités Cyber dans les Balkans occidentaux sous sa forme d'organisation internationale sera doté d'un traité fondateur, de moyens et d'organes communs, possédant la personnalité juridique.

- Articulation avec les accords ou conventions internationales existants

Du fait de son objet, l'accord n'entre pas en concurrence avec les obligations internationales de la France.¹⁹ L'adhésion de la France à l'accord portant création du C3BO n'est pas de nature à modifier les dispositions conventionnelles antérieures.

- Articulation avec le droit européen

Aucune modification du droit européen n'est nécessaire pour appliquer l'accord, et celui-ci n'emporte aucune conséquence sur le droit européen.

Pour les pays des Balkans occidentaux, le projet contribuera à accompagner leurs administrations dans l'alignement réglementaire avec l'acquis communautaire, notamment en matière de protection des réseaux et de sécurité des systèmes d'information (directives NIS et NIS 2).

Au niveau politique, l'importance du renforcement capacitaire cyber pour l'Union européenne est régulièrement souligné depuis l'adoption des conclusions du Conseil de l'UE sur les principes directeurs du renforcement capacitaire cyber en juin 2018²⁰. L'UE a plusieurs fois eu l'opportunité de développer cette vision, notamment dans la Stratégie de l'UE pour la cybersécurité de décembre 2020²¹, la Boussole stratégique, les conclusions sur la Posture cyber de l'UE de mai 2022²², mais également dans les conclusions du Conseil de l'UE sur la diplomatie numérique de l'UE de juin 2023²³.

- Articulation avec le droit interne

Aucune modification du droit interne n'est nécessaire pour appliquer l'accord.

¹⁹ Convention sur la cybercriminalité, signée à Budapest le 23 novembre 2001 (Décret n° 2006-580 du 23 mai 2006) ; 1^{er} Protocole additionnel à la Convention sur la cybercriminalité, relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (Décret n° 2006-597 du 23 mai 2006) ; Deuxième Protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et de la divulgation de preuves électroniques, fait à Strasbourg le 12 mai 2022 (dont le processus de ratification est en cours).

²⁰ Conclusions du Conseil de l'UE sur les principes directeurs du renforcement capacitaire cyber, 26 juin 2018.

²¹ Stratégie de l'UE pour la cybersécurité de décembre 2020.

²² Conclusions sur la Posture cyber de l'UE de mai 2022.

²³ Conclusions du Conseil de l'UE sur la diplomatie numérique de l'UE de juin 2023.

- **Champ d'application territorial de l'accord**

Le siège du Centre est situé à Podgorica, au Monténégro. Les conditions d'établissement du Centre seront définies dans un accord de siège. Cet accord de siège sera conclu entre le C3BO et le Monténégro dès que C3BO aura le statut d'organisation internationale. L'accord de siège définira son statut juridique et les privilèges qui lui seront accordés.

d. Conséquences financières

La France a engagé, en sa qualité de membre fondateur, des fonds permettant la création et l'établissement du Centre, en application de l'article 5.2 de l'accord : « *Les membres fondateurs fournissent le capital de départ nécessaire au fonctionnement du C3BO ainsi qu'une contribution annuelle conformément à l'article 13* ».

Ces fonds s'élèvent à 524 000 euros en 2023 et 1 172 000 euros en 2024, imputés au programme budgétaire 105 « *Action de la France en Europe et dans le Monde* »²⁴.

Le Centre ambitionne la conclusion d'un accord de contribution avec l'Union européenne à partir de 2025. La Commission européenne (via la DG Near - Direction générale du voisinage et des négociations d'élargissement) a été sollicitée en 2023 pour une contribution financière de 10 296 179 euros pour la période 2026-2028.

Par ailleurs, le renforcement capacitaire cyber aura un impact non-négligeable dans la lutte contre la criminalité financière, notamment celle qui utilise les crypto-monnaies afin de blanchir ces activités illégales.

Entre février 2023 et janvier 2024, selon les rapports d'analyse de *Chainalysis*,²⁵ il est observé dans la région des Balkans occidentaux un volume de transactions en cryptomonnaies important. Il est également noté une utilisation soutenue des plateformes d'échange (Exchangers de type Binance, Kraken) pour les cryptomonnaies sur la Blockchain.

La Serbie est située au 14^e rang dans le classement des pays européens utilisant les cryptomonnaies. Les transactions en cryptomonnaie dans ce pays sont très importantes avec un montant équivalent à 10 milliards de dollars pour la période considérée. 1,3 % de cette somme est considérée à risque, c'est-à-dire avec un lien avec des activités criminelles.

L'Albanie est au 24^e rang du classement d'utilisation des cryptomonnaies en Europe avec 3,4 milliards de dollars de transactions observées pour ma même période. Rapporté au pays, il s'agit d'un montant important. 0,5% de cette somme est considérée comme étant à risque.

²⁴ Programme 105 « *Action de la France en Europe et dans le monde* ».

²⁵ *Chainalysis* est une entreprise américaine qui détient une plateforme de données sur la blockchain et qui fournit des logiciels, des services et des recherches aux agences gouvernementales. La licence *Chainalysis* (environ 25000 euros pour un abonnement annuel) fait partie des outils indispensables aux enquêteurs pour tracer les cryptomonnaies dans la blockchain, identifier des *wallets*, et ainsi les propriétaires des cryptomonnaies. C'est un outil indispensable à la lutte contre les opérations de blanchiment via les cryptomonnaies. Cet outil fournit également des analyses annuelles sur l'état des flux et des transactions en cryptomonnaies par pays.

La Bosnie-Herzégovine est classée au 25^e rang de ce classement, avec un volume de 3,2 milliards de dollars ayant transité via des cryptomonnaies. Là encore, rapporté au pays, cela demeure des montants importants. Le taux à risque est de 0,7 %.

La Macédoine du Nord est classé au 28^e rang du classement européen pour les cryptomonnaies, avec 1,2 milliards de dollars de transactions observées. Le taux à risque est de 2 %, ce qui est élevé.

Pour le Monténégro, le montant des transactions en cryptomonnaies est de 1,1 milliards de dollars. Le Kosovo n'est pas référencé dans ce classement.²⁶

Pour l'ensemble de la région, l'activité en cryptomonnaie est considérée comme importante avec un risque élevé d'implication dans les activités criminelles. L'absence de moyens d'investigation efficaces pour la traçabilité et la saisie d'avoirs criminels en cryptomonnaies (*Wallets*) ne permet pas de connaître la part de ces volumes financiers liée aux activités de blanchiment mais les experts estiment que tout l'environnement est en place pour que le blanchiment via les crypto-actifs soient importants.

Compte tenu de cette situation, le projet de renforcement capacitaire cyber porté par le C3BO revêt toute son importance et permettra de former et de doter les agents de la région avec les outils d'investigation nécessaires afin de ne plus être aveugle en ce qui concerne les flux de crypto-actifs.

La possibilité d'augmenter le nombre de confiscations des avoirs criminels devrait également entraîner une augmentation de la redistribution de ces saisies au bénéfice du service public et des parties civiles.

L'entrée en vigueur de l'accord permettra de développer C3BO en tant que pôle régional d'expertise et de l'ouvrir dès que possible à des financements étrangers, d'une part des pays de la région, d'autre part de l'Union européenne et de ses Etats membres, afin de diminuer, à terme, la part de la contribution française.

e. Conséquences administratives

Au sein de l'organisation interministérielle, la mise en œuvre de l'accord *C3BO* mobilisera les directions des ministères suivants :

- Pour le ministère de l'Europe et des Affaires étrangères : Direction de la Coopération de Sécurité et de Défense, Direction des Affaires stratégiques de sécurité et du désarmement, Direction de l'Union européenne, Direction des affaires juridiques, Direction de l'Europe continentale

- Pour le ministère de l'Intérieur et des Outre-Mer : Direction de la coopération internationale de sécurité, Direction des Affaires européennes et internationales, Gendarmerie nationale, ComCyber MI...

²⁶ L'ensemble des données fournies ici sont issues de *Chainalysis country Brief*.

Il est convenu d'élargir prochainement la coopération interministérielle aux :

- Ministère de la justice : Section J3 du Parquet de la JUNALCO (Juridiction nationale de lutte contre la criminalité organisée) ;
- Ministère de l'économie et des finances : Direction générale des douanes et des droits indirects.

Durant les premières formations au Centre, le ComCyberMI (Commandement du ministère de l'Intérieur dans le Cyberespace), la réserve cyber de la gendarmerie nationale, ainsi que le secteur privé français (Total, HarfangLab) ont été mis à contribution dans une perspective de décloisonnement et de synergie des actions des secteurs public et privé.

f. Conséquences concernant l'égalité femmes-hommes

La stratégie en faveur de l'égalité entre les femmes et les hommes²⁷ définit les travaux que la Commission européenne entend mener dans ce domaine et décrit les objectifs stratégiques à atteindre et les mesures essentielles à prendre au cours de la période 2020-2025. Sa mise en œuvre repose sur une approche double, consistant en des mesures ciblées tendant à l'égalité entre les femmes et les hommes, combinées à une intégration renforcée de la dimension femmes-hommes dans toutes les politiques.

Parmi les objectifs poursuivis par le C3BO figurent :

- La participation accrue des femmes aux formations délivrées par et dans le Centre ;
- La promotion auprès des femmes des métiers de la cybersécurité ;
- L'engagement de la société civile (*Woman4Cyber*, *Women In Tech* et *SheLeadsTech*) dans la conception et la délivrance des programmes, en particulier les actions de sensibilisation et de communications sur les métiers du cyber ;
- La formation des équipes d'enquêtes, notamment en charge de la lutte contre le harcèlement en ligne et la pédopornographie.

En lien avec l'Union internationale des télécommunications (UIT), une formation s'est ainsi déjà tenue en septembre 2023 sur le modèle du projet « *Her CyberTracks* », initiative en trois parties intégrant des formations techniques en ligne et sur site en politique et diplomatie de cybersécurité, des formations sur les compétences générales, des cycles de mentorat, des conférences, ainsi que des événements de réseautage régionaux.

g. Conséquences sur la jeunesse

La diffusion de *curricula* universitaires français (Université Côte d'Azur) en matière de cyber sécurité, dans les universités de la région, à destination des étudiants des pays bénéficiaires, constituera un volet important de ce programme, et permettra de renforcer son impact structurel.

²⁷ Une Union de l'égalité : stratégie en faveur de l'égalité entre les hommes et les femmes 2020-2025.

Dans un cadre plus global, le renforcement des capacités cyber permettra d'améliorer la réponse judiciaire, en particulier à l'exploitation et aux abus sexuels des femmes et des enfants en ligne.

VII. Etat des signatures et ratifications

A ce stade, les partenaires slovènes ont indiqué un calendrier de ratification à l'été 2024. Le Monténégro a pour sa part signalé que la ratification pourrait intervenir dès que nécessaire s'agissant d'un projet très prioritaire pour plusieurs ministères, dont principalement le ministère des Affaires étrangères et le ministère de l'Administration publique.

ACCORD

PORTANT CRÉATION DU CENTRE DE DÉVELOPPEMENT DES CAPACITÉS CYBER DANS LES BALKANS OCCIDENTAUX (C3BO), FAIT À TIRANA LE 16 OCTOBRE 2023

PRÉAMBULE

Les Parties contractantes au présent Accord,

Considérant la signature de la lettre d'intention relative à la mise en place du Centre de développement des capacités cyber dans les Balkans occidentaux entre le ministère de l'Europe et des Affaires étrangères de la République française, le ministère des Affaires étrangères du Monténégro et le ministère des Affaires étrangères de la République de Slovénie, à Podgorica le 16 novembre 2022,

Désireuses de renforcer la stabilité et la sécurité du cyberspace dans le monde entier,

Réaffirmant leur soutien en faveur d'un cyberspace ouvert, sûr, stable, non fragmenté, pacifique et accessible à tous,

Reconnaissant que la multiplication des actes de malveillance dans le cyberspace constitue aujourd'hui l'une des principales menaces pesant sur l'environnement de sécurité régional,

Conscientes de la nécessité de renforcer la résilience des pays des Balkans occidentaux dans le domaine du cyberspace,

Soulignant la nécessité d'approfondir la coopération entre tous les acteurs régionaux pour lutter contre ces menaces,

Souhaitant créer une plateforme régionale proposant des programmes de formation avancés et pertinents aux membres clés du personnel des infrastructures essentielles, notamment publiques, dans la région, et favorisant la coopération afin d'élaborer une maquette de cours dans la sphère universitaire régionale sur les questions relatives au cyberspace,

Sont convenues de ce qui suit :

I. CRÉATION

Article premier

Définitions

Aux fins du présent Accord, les définitions suivantes s'appliquent :

- a) on entend par « Accord » le présent Accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (ci-après dénommé le « C3BO ») ;
- b) on entend par « membre fondateur » la France, le Monténégro ou la Slovénie ;
- c) on entend par « autre pays appartenant au groupe des six pays des Balkans occidentaux » l'Albanie, la Bosnie-Herzégovine, le Kosovo*, la Macédoine du Nord ou la Serbie ;
- d) on entend par « autre membre appartenant au groupe des six pays des Balkans occidentaux » l'Albanie, la Bosnie-Herzégovine, le Kosovo*, la Macédoine du Nord ou la Serbie, pour autant que le pays soit partie au présent Accord ;
- e) on entend par « autre membre » un pays ou une organisation internationale ou régionale qui n'est ni un membre fondateur ni un autre membre appartenant au groupe des six pays des Balkans occidentaux, pour autant que le pays ou l'organisation soit partie au présent Accord ;
- f) on entend par « membre du C3BO » tout membre fondateur, tout autre membre appartenant au groupe des six pays des Balkans occidentaux ou tout autre membre ;
- g) on entend par « membres du Conseil d'administration » les représentants d'un membre du C3BO ;
- h) on entend par « membres du Conseil consultatif » les représentants des membres du C3BO dont la participation au Conseil consultatif a été approuvée par le Conseil d'administration ;
- i) on entend par « agent » tout membre du personnel du C3BO ;
- j) on entend par « règlement intérieur » les dispositions fondamentales régissant le fonctionnement du C3BO adoptées par le Conseil d'administration.

* Cette désignation est sans préjudice des positions sur le statut du Kosovo et est conforme à la résolution 1244 du Conseil de sécurité des Nations Unies ainsi qu'à l'avis de la Cour internationale de Justice sur la déclaration d'indépendance du Kosovo.

Article 2

Création et statut

1. Le nom complet de l'organisation internationale est : « Centre de développement des capacités cyber dans les Balkans occidentaux » (C3BO).

2. Le C3BO est créé par le présent Accord en tant qu'organisation internationale et intergouvernementale en vertu du droit international.
3. Le C3BO jouit de la personnalité juridique internationale.

Article 3

Siège

1. Le C3BO a son siège à Podgorica (Monténégro).
2. Les conditions d'établissement du C3BO sont définies dans un accord de siège.

Article 4

Objectifs et activités

1. L'objectif du C3BO est de renforcer la cyberrésilience des Balkans occidentaux grâce à la promotion d'une culture du cyberspace par la formation et la sensibilisation, à l'approfondissement des connaissances des praticiens et à la création d'un réseau régional de coopération.
2. Les activités du C3BO sont les suivantes :
 - a) organiser des formations visant :
 - à promouvoir la culture du cyberspace ;
 - à renforcer les capacités opérationnelles,
 - à promouvoir la coopération internationale et régionale ;
 - b) faciliter la mise en commun d'expériences et l'échange d'informations et de bonnes pratiques afin de favoriser le renforcement des capacités en matière de cybersécurité ;
 - c) soutenir l'élaboration d'une maquette de cours dans la sphère universitaire régionale sur les questions relatives au cyberspace.
3. Les activités du C3BO portent notamment sur la cybersécurité, la lutte contre la cybercriminalité et la coopération internationale dans le cyberspace.

II. MEMBRES DU C3BO

Article 5

Membres fondateurs

1. Les membres fondateurs du C3BO sont la France, le Monténégro et la Slovénie.
2. Les membres fondateurs fournissent le capital de départ nécessaire au fonctionnement du C3BO ainsi qu'une contribution annuelle conformément à l'article 13.
3. Chaque membre fondateur dispose de deux représentants au Conseil d'administration.

Article 6

Autres membres appartenant au groupe des six pays des Balkans occidentaux

1. Les autres pays appartenant au groupe des six pays des Balkans occidentaux peuvent devenir membres du C3BO en adhérant au présent Accord.
2. Chaque autre membre appartenant au groupe des six pays des Balkans occidentaux dispose d'un représentant au Conseil d'administration.
3. Les autres membres appartenant au groupe des six pays des Balkans occidentaux ont l'obligation de s'acquitter d'une contribution annuelle fixée par le Conseil d'administration.
4. Si ledit membre ne s'acquitte pas de sa contribution annuelle obligatoire, le droit de vote de son représentant peut être suspendu conformément au règlement intérieur.

Article 7

Autres membres

1. D'autres pays et organisations internationales peuvent devenir membres du C3BO en adhérant au présent Accord si leur candidature est approuvée par un vote à la majorité des deux tiers au minimum du Conseil d'administration.
2. Chaque autre membre dispose d'un représentant au Conseil d'administration.
3. Les autres membres ont l'obligation de s'acquitter d'une contribution annuelle fixée par le Conseil d'administration.
4. Si ledit membre ne s'acquitte pas de sa contribution annuelle obligatoire, le droit de vote de son représentant peut être suspendu conformément au règlement intérieur.

Article 8

Suspension des droits d'un membre

Le Conseil d'administration peut suspendre tout ou partie des droits d'un membre après vote à la majorité des trois quarts dans le cadre d'une procédure déterminée par le règlement intérieur. La suspension peut être prononcée en raison du grave manquement d'un membre aux objectifs communs de cybersécurité et de stabilité du C3BO.

III. GOUVERNANCE ET ORGANISATION

Article 9

Structure du C3BO

1. Les organes principaux du C3BO sont les suivants :
 - a) le Conseil d'administration ;
 - b) le Conseil consultatif ; et
 - c) le Secrétariat.
2. Le Conseil d'administration peut créer des organes subsidiaires qu'il estime nécessaires à l'exercice de ses fonctions conformément au présent Accord.

Article 10

Conseil d'administration

1. Chaque membre fondateur dispose de deux représentants, et chaque autre membre du C3BO d'un représentant.
2. Les membres fondateurs s'informent mutuellement de la désignation de leurs représentants lors de la première session du Conseil d'administration, au plus tard trente jours après l'entrée en vigueur du présent Accord.
3. Chaque représentant dispose d'une voix.
4. Chaque représentant peut avoir un suppléant qui s'acquitte de ses responsabilités et vote à sa place en son absence.
5. Le Conseil d'administration prend ses décisions à la majorité simple, à l'exception :
 - a) de l'adoption du règlement intérieur ;
 - b) de l'admission de nouveaux membres ;
 - c) de l'approbation d'amendements au présent Accord ;qui sont prononcées à la majorité qualifiée, par un vote à la majorité des deux tiers au minimum. Conformément à l'article 8 du présent Accord, la suspension des droits d'un membre est prononcée à la majorité des trois quarts.
6. Le Conseil d'administration :
 - a) supervise les activités du C3BO ;
 - b) adopte le programme de travail et le rapport final sur le programme, ainsi que le budget annuel ;
 - c) adopte le programme final et les états financiers ;
 - d) nomme le directeur général, le directeur du programme et le commissaire aux comptes ;
 - e) donne décharge au directeur général et au directeur du programme ;
 - f) nomme les membres du Conseil consultatif ;
 - g) nomme des membres supplémentaires au sein du Conseil consultatif ;
 - h) adopte le règlement intérieur et les autres règlements internes du C3BO ;
 - i) approuve les amendements au présent Accord ;
 - j) autorise le directeur général à négocier des accords internationaux, au nom du C3BO ;
 - k) approuve la conclusion d'accords internationaux ;
 - l) s'acquitte de toute autre fonction ou responsabilité en vertu du présent Accord et du règlement intérieur.

Article 11

Conseil consultatif

1. Chaque membre du C3BO peut disposer d'un représentant au Conseil consultatif.
2. Si le Conseil consultatif travaille en sous-comités, chaque membre du C3BO peut disposer d'un représentant dans chacun des sous-comités.
3. Des membres supplémentaires du Conseil consultatif peuvent être désignés par un vote du Conseil d'administration à la majorité simple au minimum.

4. Le directeur du programme préside le Conseil consultatif, présente au Conseil d'administration le plan de programme et le rapport final sur le programme pour adoption, procède au recrutement d'experts et met en œuvre le programme.
5. Le Conseil consultatif élabore le programme de travail ainsi qu'un plan pluriannuel de développement du programme.

Article 12

Secrétariat

1. Le directeur général est le représentant légal du C3BO.
2. Le Conseil d'administration désigne le directeur général dans le cadre d'une procédure de sélection par mise en compétition par un vote à la majorité simple au minimum.
3. Trois membres du Conseil d'administration, représentant chacun un membre fondateur, exercent les droits et les obligations d'un employeur dans la relation de travail liant le C3BO et le directeur général ; ils représentent collectivement le C3BO lorsque le directeur général n'a pas été nommé. Ces trois membres du Conseil d'administration peuvent nommer un directeur général adjoint.
4. Le directeur général présente au Conseil d'administration des propositions concernant le budget annuel et le rapport financier ainsi que des amendements au règlement intérieur et aux autres règlements internes.
5. Le directeur général peut conclure des contrats de recrutement d'agents conformément au droit du travail monténégrin, si le budget annuel adopté le prévoit.
6. Le directeur peut également conclure des contrats avec les agents affectés au C3BO conformément aux règlements nationaux et du C3BO relatifs à l'affectation d'agents des pays membres du C3BO, si le budget annuel adopté le prévoit.

IV. FINANCEMENT

Article 13

Ressources financières et responsabilité

1. Les membres du C3BO sont responsables conjointement et solidairement de la prise en charge des coûts fixes du C3BO.
2. Le C3BO est financé par des contributions, financières et en nature, fournies par ses membres, par des partenaires et par des bailleurs de fonds.
3. Le Conseil d'administration fixe le montant des contributions annuelles dues par les membres.

V. RÈGLEMENT INTÉRIEUR ET AUTRES RÈGLEMENTS INTERNES

Article 14

Règlement intérieur et autres règlements internes

1. Le Conseil d'administration adopte le règlement intérieur du C3BO à la majorité des deux tiers.
2. Le règlement intérieur est adopté lors de la première session du Conseil d'administration suivant la création du C3BO.
3. Le Conseil d'administration peut adopter des règlements internes supplémentaires dans les mêmes conditions d'adoption que le règlement intérieur.

VI. TRAITEMENT DES DONNÉES ET HABILITATION DE SÉCURITÉ

Article 15

Traitement des données

Les règles relatives à la protection des données applicables au C3BO sont détaillées par le règlement intérieur adopté par le Conseil d'administration, en conformité avec les obligations internationales et, le cas échéant, européennes des Parties.

Article 16

Habilitation de sécurité

Les candidats ayant satisfait aux exigences de recrutement du C3BO doivent se soumettre à une procédure d'habilitation de sécurité conduite par les autorités compétentes des membres fondateurs. Ladite procédure est menée conformément au droit interne des membres fondateurs.

VII. DISPOSITIONS FINALES

Article 17

Réserve

Aucune réserve ne peut être faite au présent Accord.

Article 18

Signature, ratification, approbation et adhésion

1. Le présent Accord est ouvert à la signature des trois membres fondateurs.
2. Le présent Accord est soumis à ratification ou approbation par les membres fondateurs, conformément à leurs exigences juridiques respectives.
3. Le présent Accord est ouvert à l'adhésion des autres pays appartenant au groupe des six pays des Balkans occidentaux.
4. Le présent Accord est ouvert à l'adhésion d'autres Etats et organisations internationales sous réserve de l'autorisation écrite préalable du Conseil d'administration.
5. Les instruments de ratification, d'approbation ou d'adhésion sont déposés auprès du dépositaire.

Article 19

Entrée en vigueur

1. Le présent Accord entre en vigueur le trentième jour qui suit la date de dépôt du dernier instrument de ratification ou d'approbation auprès du dépositaire par les membres fondateurs.
2. Pour chaque Etat ou organisation internationale adhérant au présent Accord, celui-ci entre en vigueur à la date de dépôt de l'instrument correspondant.

Article 20

Amendements

1. Tout membre du C3BO peut proposer au Conseil d'administration des amendements au présent Accord.
2. Un amendement entre en vigueur pour tous les membres du C3BO :
 - a) après son approbation par le Conseil d'administration par un vote à la majorité des deux tiers ; et
 - b) dès lors que tous les membres du C3BO ont consenti à être liés par ledit amendement, conformément à leurs procédures juridiques internes respectives, par le dépôt d'un instrument de ratification, d'acceptation, d'approbation ou d'adhésion auprès du dépositaire.
3. Le dépositaire informe les membres de l'entrée en vigueur de l'amendement.

Article 21

Retrait

1. Après l'entrée en vigueur du présent Accord, toute Partie contractante peut s'en retirer en adressant une notification écrite au dépositaire du présent Accord, qui en informe immédiatement les autres membres du C3BO.
2. Le retrait prend effet six mois après la date de réception par le dépositaire de ladite notification écrite.
3. A moins que tous les membres demeurant partie au C3BO n'en conviennent autrement, le retrait ne libère pas le membre qui se retire de ses obligations financières au titre de l'exercice au cours duquel le retrait a été notifié.

Article 22

Dénonciation

1. Le présent Accord peut être dénoncé par consentement mutuel des membres du C3BO.
2. En cas de dénonciation du présent Accord, le C3BO s'efforce de mener à bien les projets en cours.
3. Une fois ces activités menées à bien, le patrimoine propre du C3BO est transféré aux membres du C3BO au prorata de leurs investissements et de leurs contributions annuelles.
4. La liquidation du C3BO est effective un an au maximum à partir de la dénonciation.

Article 23

Règlement des différends

1. Tout différend relatif à l'interprétation ou à la mise en œuvre du présent Accord, y compris à l'interprétation ou à la mise en œuvre des droits et obligations respectifs des membres du C3BO, est réglé à l'amiable par voie de consultations et de négociations.
2. Tout différend non réglé par voie de négociations ou par un autre mode de règlement arrêté d'un commun accord est soumis à un tribunal d'arbitrage composé de trois arbitres dont la décision est définitive et obligatoire pour les parties. Chaque partie au différend désigne un arbitre ; les deux arbitres ainsi désignés en désignent un troisième d'un commun accord, qui exerce les fonctions de président du tribunal. Le président du tribunal ne peut être ressortissant d'une des parties au différend, ni avoir sa résidence habituelle sur le territoire de l'une de ces parties, ni se trouver au service de l'une d'elles, ni s'être déjà occupé de l'affaire à un autre titre. En cas de différend entre plus de deux parties, les parties qui font cause commune nomment un arbitre d'un commun accord. Il est pourvu à tout siège vacant de la manière prévue pour la nomination initiale. Si les parties ne s'accordent pas sur l'objet du différend avant que le président du tribunal d'arbitrage ne soit désigné, il appartient au tribunal d'arbitrage de le déterminer.

Article 24

Dépositaire

1. Le gouvernement du Monténégro, par l'intermédiaire du Ministère des Affaires étrangères, est le dépositaire du présent Accord.
2. Après l'entrée en vigueur du présent Accord, le dépositaire en assure l'enregistrement auprès du Secrétariat de l'ONU, conformément à l'article 102 de la Charte des Nations Unies.
3. Le présent Accord, établi en un seul exemplaire original en langues française et anglaise, est déposé auprès du dépositaire, qui en remet une copie certifiée conforme à chaque membre fondateur et à tout Etat ou organisation internationale ou régionale souhaitant adhérer au présent Accord.

EN FOI DE QUOI, les soussignés, dûment autorisés à cet effet, ont signé le présent Accord.

Fait à Tirana le 16 octobre 2023, en langues française et anglaise, les deux textes faisant également foi.

POUR
LA RÉPUBLIQUE FRANÇAISE
La secrétaire d'État
chargée de l'Europe
Laurence Boone

POUR
LE MONTÉNÉGRO
Le Président du
Gouvernement
Dritan Abazović

POUR
LA RÉPUBLIQUE DE SLOVÉNIE
La Présidente
Nataša Pirc Musar