

N° 1377

# ASSEMBLÉE NATIONALE

CONSTITUTION DU 4 OCTOBRE 1958

DIX-SEPTIÈME LÉGISLATURE

---

Enregistré à la Présidence de l'Assemblée nationale le 7 mai 2025.

## RAPPORT

FAIT

AU NOM DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES SUR LE PROJET DE LOI,  
*adopté par le Sénat, autorisant l'approbation de l'accord portant création du*  
**Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO)**

PAR MME MARINE HAMELET

Députée

---

AVEC

**EN ANNEXE**  
**LE TEXTE DE LA COMMISSION**  
**DES AFFAIRES ÉTRANGÈRES**

---

Voir les numéros :

Assemblée nationale : **944.**

Sénat : **166, 284, 285 et T.A. 50 (2024-2025).**



## SOMMAIRE

---

	Pages
<b>INTRODUCTION .....</b>	<b>5</b>
<b>I. LE CENTRE DE DÉVELOPPEMENT DES CAPACITÉS CYBER DANS LES BALKANS OCCIDENTAUX (C3BO) : UNE INITIATIVE FRANÇAISE ORIGINALE DANS UNE RÉGION MARQUÉE PAR LA CYBERCRIMINALITÉ .....</b>	<b>7</b>
<b>A. UNE RÉGION À L'ÉQUILIBRE FRAGILE .....</b>	<b>7</b>
1. Rappel historique .....	7
2. Des tensions persistantes .....	8
3. Des défis institutionnels et sécuritaires.....	8
<b>B. UNE CIBLE DE CHOIX POUR LES CYBERCRIMINELS, AVEC DES IMPACTS POTENTIELS POUR LA FRANCE.....</b>	<b>9</b>
1. Une forte vulnérabilité à la cybercriminalité .....	9
2. Des conséquences éventuelles en France.....	10
<b>C. LE C3BO : UN TOURNANT POUR NOS COOPÉRATIONS BILATÉRALES ? .....</b>	<b>11</b>
1. Un réengagement de la France dans la région .....	11
2. La création du centre en novembre 2022 : une initiative de cyberdiplomatie originale.....	12
3. Les premières actions du centre.....	14
<b>II. UN ACCORD QUI TRANSFORME LE C3BO EN ORGANISATION INTERNATIONALE SANS RÉGLER LA QUESTION FINANCIÈRE .....</b>	<b>16</b>
<b>A. LES DISPOSITIONS DE L'ACCORD .....</b>	<b>16</b>
1. Le statut et les missions du C3BO .....	16
2. Les membres .....	17
3. L'organisation et le fonctionnement .....	18
4. Les clauses finales .....	19

B. UN TEXTE UTILE MAIS QUI NE PERMET PAS ENCORE DE RÉDUIRE L'ENGAGEMENT FINANCIER DE LA FRANCE .....	19
1. Le statut d'organisation internationale renforce et légitime le centre.....	19
2. Une contribution financière française trop élevée .....	20
<b>EXAMEN EN COMMISSION .....</b>	<b>21</b>
<b>ANNEXE 1 : TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES.....</b>	<b>35</b>
<b>ANNEXE 2 : LISTE DES PERSONNES AUDITIONNÉES PAR LA RAPPORTEURE .....</b>	<b>37</b>
<b>ANNEXE 3 : FUTURE ORGANISATION DU C3BO .....</b>	<b>39</b>
<b>ANNEXE 4 : STRATÉGIE FRANÇAISE POUR LES BALKANS OCCIDENTAUX (VERSION D'OCTOBRE 2023) .....</b>	<b>41</b>

## INTRODUCTION

La commission des affaires étrangères de l'Assemblée nationale est saisie du projet de loi n° 944 autorisant l'approbation de l'accord entre la France, le Monténégro et la Slovénie portant création du centre de développement des capacités cyber dans les Balkans occidentaux (C3BO). Cet accord a été signé par la secrétaire d'État chargée de l'Europe, Mme Laurence Boone, le président du gouvernement du Monténégro, M. Dristan Abazovic, et la présidente de la République de Slovénie, Mme Natasa Pirc Musar, le 16 octobre 2023, à Tirana.

Le C3BO représente une initiative forte de cyberdiplomatie, dans une région vulnérable à la cybercriminalité. En renforçant la cyberrésilience de ses partenaires des Balkans occidentaux, la France espère améliorer sa propre sécurité. Mais le C3BO permet surtout de renforcer nos relations bilatérales dans une région stratégique.

En donnant le statut d'organisation internationale au C3BO, l'accord du 16 octobre 2023 pourrait permettre d'attirer de nouveaux partenariats, voire de nouveaux membres. La rapporteure regrette que seul un pays des Balkans occidentaux soit aujourd'hui membre du centre.

De plus, la rapporteure constate l'importance de la contribution financière de la France – près d'un million d'euros en 2025 – et appelle à une réduction de cet engagement financier, en partageant les coûts avec les bénéficiaires et avec d'autres partenaires étrangers. La répartition financière actuelle apparaît en effet déséquilibrée.

Après le Sénat, le 12 février 2025, l'Assemblée est invitée à autoriser l'approbation de ce texte en adoptant le projet de loi à cet effet. La Slovénie et le Monténégro ont pour leur part achevé leurs procédures internes.



## I. LE CENTRE DE DÉVELOPPEMENT DES CAPACITÉS CYBER DANS LES BALKANS OCCIDENTAUX (C3BO) : UNE INITIATIVE FRANÇAISE ORIGINALE DANS UNE RÉGION MARQUÉE PAR LA CYBERCRIMINALITÉ

### A. UNE RÉGION À L'ÉQUILIBRE FRAGILE

Les Balkans occidentaux comprennent six pays : l'Albanie, la Bosnie-Herzégovine, le Kosovo, la Macédoine du Nord, le Monténégro et la Serbie. Ils regroupent environ 17 millions d'habitants sur 215 000 km<sup>2</sup>, soit une surface proche de celle de la Roumanie ou du Royaume-Uni.

Sous la 16<sup>e</sup> législature, la rapporteure et le député Frédéric Petit avaient publié un rapport d'information sur un déplacement en Bosnie-Herzégovine, en Serbie et en Albanie effectué du 12 au 17 mars 2023. Ce rapport dressait un état des lieux de la situation dans les Balkans occidentaux. Les défis identifiés apparaissent toujours d'actualité : *« consolidation de la démocratie et de l'État de droit, maîtrise des risques sécuritaires, transition énergétique, recul démographique, sans oublier la persistance de foyers de crise internes qui peuvent être déstabilisateurs »* <sup>(1)</sup>.

Ainsi, la vulnérabilité de la région des Balkans occidentaux face à la cybercriminalité ne peut être appréhendée sans rappeler la profondeur des tensions qui continuent de structurer cet espace géopolitique.

#### 1. Rappel historique

Les Balkans occidentaux portent encore l'héritage de l'éclatement brutal de la Yougoslavie dans les années 1990.

Parmi les « guerres de Yougoslavie », la guerre de Bosnie (1992-1995) a provoqué la mort de presque 100 000 personnes (dont 40 % de civils) et laissé des fractures profondes. Bien que les combats aient officiellement cessé avec la signature des accords de Dayton à Paris le 14 décembre 1995, le conflit a en effet durablement marqué les mémoires et ancré certaines divisions ethniques, confessionnelles et territoriales.

La guerre du Kosovo (1998-1999), née de la volonté d'indépendance de la majorité albanaise du Kosovo face à Belgrade, a également marqué la région. Ce territoire a finalement proclamé unilatéralement son indépendance en 2008, mais celle-ci fait l'objet d'une reconnaissance partielle de la communauté internationale <sup>(2)</sup>.

---

(1) Page 5 du rapport, disponible sur le site Internet de l'Assemblée nationale : [https://www.assemblee-nationale.fr/dyn/16/rapports/cion\\_afetr/l16b1227\\_rapport-information.pdf](https://www.assemblee-nationale.fr/dyn/16/rapports/cion_afetr/l16b1227_rapport-information.pdf).

(2) Près de cent dix pays, dont la France, reconnaissent cette indépendance. Parmi les pays qui ne la reconnaissent pas figurent, outre la Serbie, cinq membres de l'Union européenne (Chypre, Espagne, Grèce, Roumanie, Slovaquie), la Russie et la Chine.

## 2. Des tensions persistantes

La reconnaissance du Kosovo comme État indépendant demeure un sujet de tension majeur dans la région. Il implique aussi des acteurs étrangers puisque l'Organisation du traité de l'Atlantique Nord (OTAN) garantit toujours la sécurité du Kosovo (à travers la Force pour le Kosovo – KFOR) et que la Russie soutient les intérêts serbes.

En parallèle, d'autres différends bilatéraux persistent : contestation de la langue macédonienne par la Bulgarie, litiges mémoriels entre la Serbie et la Croatie et tensions multiformes entre la Grèce et l'Albanie (questions des minorités, de la frontière maritime, de l'intégration de l'Albanie à l'Union européenne).

Le facteur identitaire, fréquemment mobilisé par les acteurs politiques locaux, a également contribué à des recompositions institutionnelles internes aux États qui ne favorisent pas toujours la stabilité ni la réconciliation. C'est le cas de la Bosnie-Herzégovine, dont l'organisation repose sur un principe de citoyenneté ethnique, qui crée une inégalité de droits entre les citoyens issus des trois peuples constitutifs (Bosniaques, Serbes et Croates) et ceux qui ne le sont pas (Roms, Juifs, Slovènes, *etc.*).

Néanmoins, la région ne peut pas être appréhendée sous le seul prisme des tensions puisque des initiatives de coopération bilatérales et régionales existent et doivent être saluées, dont le conseil de coopération régional (*Regional Cooperation Council* – RCC) <sup>(1)</sup>.

## 3. Des défis institutionnels et sécuritaires

Malgré le lancement, dès le début des années 2000, de réformes démocratiques dans les pays des Balkans occidentaux – notamment à travers les accords de stabilisation et d'association (ASA) –, les institutions de ceux-ci demeurent trop souvent fragiles et marquées par des défaillances structurelles.

Dans une communication sur la politique d'élargissement de l'Union européenne publiée en octobre 2024, la Commission européenne rappelle par exemple que des lacunes subsistent encore en matière de d'efficacité et d'indépendance des systèmes judiciaires, citant en particulier « *les arriérés judiciaires, les difficultés à occuper les postes vacants et les financements insuffisants* », mais aussi « *les tentatives d'ingérence politique* » <sup>(2)</sup>.

La corruption alimente des dynamiques de pouvoir déstabilisatrices ainsi qu'un sentiment général de méfiance envers les autorités. En Serbie, des

---

(1) Voir les pages 20 à 22 du rapport d'information de 2023.

(2) « Communication de 2024 sur la politique d'élargissement de l'UE », *Commission européenne*, octobre 2024.



manifestations d'origine étudiantes dénoncent depuis le mois de novembre 2024 <sup>(1)</sup> la corruption, le népotisme et le clientélisme dans le système politique serbe.

La corruption est parfois alimentée par des réseaux de criminalité organisée. La région est confrontée à de nombreux trafics (armes, stupéfiants, migrations, véhicules volés, *etc.*), avec des effets majeurs pour la sécurité des pays, mais aussi pour tout le continent européen <sup>(2)</sup>.

## **B. UNE CIBLE DE CHOIX POUR LES CYBERCRIMINELS, AVEC DES IMPACTS POTENTIELS POUR LA FRANCE**

### **1. Une forte vulnérabilité à la cybercriminalité**

Les Balkans occidentaux sont confrontés à une importante menace cyber. En 2022, l'Albanie et le Monténégro ont notamment subi des attaques d'ampleur contre des infrastructures et des systèmes gouvernementaux. En Albanie, ces attaques ont d'abord touché des données gouvernementales, en juillet, puis un système informatique des douanes, en septembre. Elles ont été attribuées publiquement par l'Albanie et par les États-Unis à l'Iran. Au Monténégro, l'attaque a impacté en profondeur plusieurs administrations publiques et le pays a sollicité une aide internationale, à laquelle les États-Unis et la France ont répondu. L'attaque est considérée comme étant d'origine russe et liée au soutien public du pays à l'Ukraine.

En outre, en décembre 2023, les autorités albanaises ont annoncé une attaque contre le site du Parlement, puis, en février 2024, contre l'institut national des statistiques.

La région, à l'exception de la Serbie <sup>(3)</sup> et dans une moindre mesure de l'Albanie, apparaît particulièrement vulnérable à ces attaques en raison du développement rapide du numérique sans que la population ait été suffisamment sensibilisée aux enjeux de cybersécurité, mais aussi des difficultés pour recruter et fidéliser des personnels spécialisés.

En outre, certains pays ont pu se reposer sur des compétences étrangères. C'est le cas du Monténégro qui a longtemps confié sa cybersécurité aux États-Unis. Or, les contrats des experts américains placés auprès de l'administration monténégrine n'auraient pas été renouvelés par l'administration du président Donald Trump.

En parallèle, les ambitions européennes des pays de la région les exposent aux tentatives de déstabilisation étrangères, et en particulier aux attaques de la

---

*(1) Les premières manifestations ont débuté après l'effondrement d'un auvent de la gare de Novi Sad, le 1<sup>er</sup> novembre 2024. Cet accident, qui a provoqué la mort de 14 personnes, résulterait de malfaçons liées à la corruption et à des négligences dans la rénovation de la gare.*

*(2) Voir les pages 23 à 25 du rapport d'information de 2023.*

*(3) La Serbie a subi peu de cyberattaques, hormis une en 2024 portant sur le cadastre.*

Russie. Les cyberattaques s'inscrivent alors dans le cadre plus général de la guerre hybride.

L'absence d'écosystème de cybersécurité, notamment privé, ferait également peser le risque d'une valorisation criminelle des quelques compétences disponibles sur le marché. Ainsi, la société Cytrox AD, filiale de d'Intellexa basée en Macédoine du Nord, a joué un rôle clé dans la production du logiciel espion Predator <sup>(1)</sup>.

Face à cette menace cyber, certains pays ont déjà adapté leur cadre réglementaire. Depuis 2015, la Serbie a adopté une loi sur la cybersécurité et renforcé son dispositif national. L'Albanie dispose de capacités propres et de moyens de formation. Enfin, le Monténégro devrait adopter prochainement une loi sur la cybersécurité et a annoncé la création d'une agence nationale de cybersécurité en 2025, en complément d'autres initiatives telles que le C3BO.

Pour leur part, le Kosovo et la Macédoine du Nord, avancent plus timidement. Le Kosovo travaille par exemple à l'élaboration d'une stratégie cyber et d'une loi afférente.

Enfin, la Bosnie-Herzégovine marque un retard certain. Le pays ne dispose pas de centre de réponse aux incidents cyber et ne prévoit pas de projet de loi dédié à la cybersécurité.

## **2. Des conséquences éventuelles en France**

Selon le ministère de l'Europe et des affaires étrangères (MEAE), l'espace cyber étant ouvert, sans frontière, la France doit éviter que la cybercriminalité se développe dans d'autres pays, et plus particulièrement au voisinage de l'Union européenne. En effet, elle limitera ainsi les attaques sur ses citoyens menées depuis l'étranger.

Par ailleurs, le cyber sert toutes les formes de criminalité. Les narcotrafiquants utilisent par exemple de plus en plus Internet et l'Internet caché (*dark web*) pour leurs activités, et ils réalisent aussi parfois des cyberattaques pour diversifier leurs sources de revenus. Limiter le développement de la cybercriminalité dans les Balkans permettrait ainsi de limiter d'autres formes de criminalité dans la région ou sur le sol français.

Enfin, la France partage des réseaux numériques et des informations sensibles avec des pays de la zone. C'est le cas des réseaux OTAN pour les pays membres de l'organisation : l'Albanie, le Monténégro et la Macédoine du Nord <sup>(2)</sup>.

---

(1) Le 18 juillet 2023, Cytrox AD a été ajoutée à liste Entity du Département du Commerce américain pour avoir vendu des « exploits cybernétiques » utilisés pour obtenir des accès à des systèmes d'information, et le 5 mars 2024, sur la liste des désignations du bureau de contrôle des actifs étrangers (Office of Foreign Assets Control, OFAC) du Département du Trésor.

(2) L'Albanie est devenue membre en 2009, suivie par le Monténégro en 2017 et la Macédoine du Nord en 2020.

## C. LE C3BO : UN TOURNANT POUR NOS COOPÉRATIONS BILATÉRALES ?

### 1. Un réengagement de la France dans la région

Si la France était traditionnellement engagée dans les Balkans occidentaux – elle dispose d’ailleurs d’une ambassade dans chacun des pays – en promouvant notamment la stabilité régionale et son ancrage européen <sup>(1)</sup>, elle démontre une volonté de s’y réengager depuis quelques années. La Stratégie française pour les Balkans occidentaux publiée en 2019 en témoigne.

#### **La Stratégie française pour les Balkans occidentaux (version initiale)**

Dans sa version publiée en mai 2019, cette stratégie devait permettre à la France de « *s’engage[r] davantage pour la stabilisation des six pays des Balkans occidentaux non membres de l’Union européenne, pour leur développement économique et social et pour le renforcement de l’État de droit* ».

Elle comportait trois grands axes :

- l’intensification des relations politiques avec les pays de la région, avec des visites du président de la République, du gouvernement et des parlementaires ;
- le renforcement de la coopération bilatérale avec les pays de la région dans quatre domaines : le développement économique et social par l’intervention de l’Agence française de développement (AFD), la sécurité, la justice et la défense ;
- un appui et un complément à l’action de l’Union européenne pour soutenir le rapprochement européen de la région.

La cybersécurité n’était pas mentionnée dans le texte.

La Stratégie publiée en 2019, a été actualisée en octobre 2023 pour prendre en compte trois évolutions : « *la guerre d’agression russe en Ukraine et l’accentuation des difficultés économiques et sociales dans la région (...)* », « *l’évolution de la politique d’élargissement de l’Union européenne (...)* » et « *la persistance, voire l’aggravation des crises régionales requérant l’engagement de la France au plus haut niveau afin d’apporter des propositions de résolution des différends* ».

Le nouveau texte précise désormais que la France « *entend renforcer sa coopération bilatérale avec tous les pays de la région et sa contribution à la coopération régionale, avec plusieurs priorités dont i) la mise en œuvre de l’Agenda vert et la transition énergétique et numérique ii) la lutte contre la désinformation et les menaces cyber, iii) le soutien à la société civile, iv) l’appui aux administrations, présumé indispensable à la réussite des réformes dans le cadre du processus d’adhésion* ».

---

(1) La position officielle de la France est le soutien à la perspective d’adhésion de ces États à l’Union européenne, tout en rappelant les critères d’adhésion, notamment en matière d’État de droit et de lutte contre la corruption.

Les mesures concrètes réalisées ou programmées par le ministère ont alors été davantage détaillées que dans la version précédente, ce qui démontre une intensification des actions réalisées <sup>(1)</sup>, et un cinquième domaine de coopération a été identifié : « *la culture, l'éducation, la langue française et la jeunesse* ». L'axe qui visait « *à appuyer et à compléter l'action de l'Union européenne pour soutenir le rapprochement européen de la région* », a quant à lui été supprimé, même si le document appelle une intégration des pays des Balkans occidentaux dans l'Union européenne. La France a défendu un processus plus progressif, avec les critères dits « intermédiaires », mais sans abandonner l'idée d'un élargissement de l'Union à ces pays.

En parallèle, depuis octobre 2023, un poste d'envoyé spécial pour la région a été créé <sup>(2)</sup>.

La rapporteure a pu auditionner l'ambassadrice de France au Monténégro, Mme Anne-Marie Maskay. La relation bilatérale franco-monténégroise s'est nettement renforcée depuis les élections présidentielles et législatives de 2023. L'ambassadrice évoque même une « nouvelle ère » pour la relation bilatérale, illustrée par de nombreuses visites officielles. Outre le cyber, la coopération est forte dans les domaines de la défense <sup>(3)</sup>, de la santé, des infrastructures de transport et portuaires et de l'environnement. Un projet d'accord sur la coopération technologique est en cours d'élaboration.

Enfin, la France entretient également d'excellentes relations avec la Slovénie, un pays issu de l'ex-Yougoslavie, membre de l'Union européenne et de l'OTAN depuis 2004. Sur le plan économique, plus d'une centaine d'entreprises françaises sont par exemple implantées en Slovénie. Sur le plan diplomatique, les deux pays partagent souvent des analyses communes et la France apprécie l'expertise régionale slovène sur les Balkans <sup>(4)</sup>.

## **2. La création du centre en novembre 2022 : une initiative de cyberdiplomatie originale**

Le centre de développement de capacités cyber dans les Balkans occidentaux (*Western Balkans Cyber Capacity Centre*, WB3C), surnommé le

---

(1) Pour le premier de domaine de coopération, qui s'intitule désormais « présence et influence économique, notamment avec l'intervention de l'AFD », le texte mentionne par exemple cinq accords intergouvernementaux signés depuis 2019 pour permettre l'intervention de l'AFD, la création de douze postes d'experts techniques régionaux au sein des administrations des pays de la région, l'augmentation des échanges commerciaux avec les Balkans occidentaux de 77 % en cinq ans et la réimplantation prochaine d'un bureau Business France en Grèce, ayant compétence sur les Balkans occidentaux.

(2) Ce poste est actuellement occupé par M. René Troccaz.

(3) Dans le domaine de la défense, un accord intergouvernemental a été signé à Paris le 3 avril 2024. Il a permis la signature d'un contrat portant sur la fourniture de deux patrouilleurs de haute mer à la marine monténégroise par la société Kership, en novembre 2024.

(4) Le 8 janvier 2024, le partenariat stratégique franco-slovène a été renouvelé. Il s'accompagne d'un plan d'action triennal pour la période 2024-2027.

« C3BO », a été créé par un mémorandum signé par la France, le Monténégro et la Slovénie le 16 novembre 2022.

La France et la Slovénie – directement intéressée par la sécurité de son voisinage immédiat <sup>(1)</sup> – avaient au préalable recherché conjointement sous le format « équipe Europe » <sup>(2)</sup>, un troisième membre fondateur, appartenant directement aux Balkans occidentaux. Le Monténégro est apparu comme le candidat présentant le plus de garanties techniques et logistiques, la plus grande motivation, mais aussi comme pouvant jouer un rôle stabilisateur dans la région.

Paradoxalement, ce centre ne résultait qu’indirectement de la Stratégie française pour les Balkans occidentaux, puisque le texte de 2019 ne mentionnait ni le projet, ni même la menace cyber dans les domaines de coopération « sécurité » ou « défense ». Le C3BO et la menace cyber ont néanmoins été intégrés depuis dans la version d’octobre 2023, dans le domaine « sécurité ».

Le C3BO semble donc relever avant tout de la cyberdiplomatie française, théorisée progressivement par plusieurs textes, dont la Stratégie internationale de la France pour le numérique publiée en 2017, la Revue stratégique de cyberdéfense publiée en 2018 et la Revue nationale stratégique (RNS) de 2022.

Si la cyberdiplomatie française se développe, seul un autre dispositif prévoyait un centre d’expertise régionale : l’École nationale cyber à vocation régionale (ENVR Cyber) de Dakar, au Sénégal.

La cyberdiplomatie française a notamment pour objectif la cyberrésilience de ses partenaires. En effet, selon la RNS, « *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* » <sup>(3)</sup>. En contribuant au renforcement des capacités d’un autre État, la France souhaite renforcer sa propre sécurité. Elle espère également bénéficier en retour de coopérations dans la lutte contre la cybercriminalité, d’échanges de renseignements et plus simplement, améliorer la relation bilatérale avec l’État partenaire. Enfin, ce type de coopération peut permettre de vendre des services d’entreprises françaises à l’étranger.

Pour la rapporteure, le C3BO ne doit pas être compris comme contribuant à préparer les pays des Balkans occidentaux à une adhésion à l’Union européenne, comme l’affirme officiellement le pouvoir exécutif français – notamment en les rapprochant de la directive *Network and Informative Security* dite « NIS 2 ». Le C3BO doit être considéré uniquement comme une occasion d’approfondir nos

---

(1) La Slovénie mène une politique active de soutien envers ses voisins des Balkans occidentaux, auxquels elle dédie la majeure partie de son aide au développement. Ljubljana est généralement bien perçue dans la région, en raison de son histoire commune avec les pays des Balkans occidentaux (sans conflits hérités et pendants) et de l’exemple de stabilité et de prospérité qu’elle représente.

(2) Ce format permettait de bénéficier de financements de l’Union européenne, tout en mettant en commun les réseaux diplomatiques français et slovène.

(3) Revue nationale stratégique, page 40.

relations bilatérales dans un domaine stratégique, sans inclure de perspective d'élargissement de l'Union européenne.

### 3. Les premières actions du centre

Le centre C3BO a mis en œuvre ses premières actions de formation dès le mois de mai 2023 au sein de l'Université du Monténégro. S'il n'a proposé que cinq formations en 2023, il en a réalisé vingt et une en 2024, bénéficiant à environ 400 stagiaires, et en prévoit trente-cinq, pour environ 600 stagiaires, en 2025 <sup>(1)</sup>.

Ces formations se répartissent en trois domaines distincts : la lutte contre la cybercriminalité (60 % des formations en 2024, 40 % prévues en 2025), la cybersécurité (30 % en 2024, 40 % en 2025) et la cyberdiplomatie (10 % en 2024, 20 % en 2025). Ces derniers sont ensuite déclinés en programmes d'enseignement <sup>(2)</sup>.

Les formations du C3BO ont déjà bénéficié à l'Albanie, à la Bosnie-Herzégovine, au Kosovo, à la Macédoine du Nord, au Monténégro et à la Serbie, mais aussi à la Moldavie. Une réflexion est en cours pour en faire profiter l'Ukraine.

La direction de la coopération de sécurité et de défense (DCSD) du MEAE déploie trois coopérants français sur place et la Slovénie trois personnes recrutées localement, auxquelles s'ajoutera une diplomate à partir de 2025.

Les formations reposent principalement sur la contribution d'acteurs français du cyber, tels que le ComCyberMI, la réserve cyber de la gendarmerie nationale, ainsi que certaines entreprises (Total Energies, HarfangLab). Le centre collabore toutefois aussi avec d'autres projets cyber dans la région, tels que les programmes *Cyber Balkans*, mis en œuvre par l'agence estonienne eGovernance Academy et financé par l'Union européenne, et *Cyber SEE* du Conseil de l'Europe, ainsi qu'avec d'autres organisations internationales et agence spécialisées, telles que l'Union internationale de télécommunications (UIT) et le Centre national de cybersécurité néerlandais (National cybersecurity centre, NCSC).

Le C3BO est complémentaire du projet, soutenu par le États-Unis, de création d'une agence nationale de cybersécurité au Monténégro pour protéger les infrastructures critiques et les ressources stratégiques du pays face aux cyberattaques. À la date de rédaction du rapport, la pérennité du projet n'était

---

(1) Une licence en criminalité numérique dispensée par l'Université de Technologie de Troyes en onze semaines, devrait également être proposée.

(2) Par exemple, en matière de lutte contre la cybercriminalité, il existe plusieurs programmes aux thématiques proches : un sur la protection des enfants contre les délits en ligne, sur les cryptomonnaies et sur la collaboration transfrontalière ; un pour former les services répressifs aux nouveaux enjeux de la cybercriminalité ; un sur la nouvelle typologie des crimes opérant dans le cyber, sur la manière d'exploiter des preuves numériques et sur les enjeux de la cybercriminalité financière ; mais aussi un programme d'un an sur la criminalistique numérique pour les enquêteurs de police.

néanmoins pas garantie, la nouvelle administration américaine ayant suspendu les activités de renforcement des capacités cyber.

## II. UN ACCORD QUI TRANSFORME LE C3BO EN ORGANISATION INTERNATIONALE SANS RÉGLER LA QUESTION FINANCIÈRE

L'accord du 16 octobre 2023 a été signé à Tirana, en Albanie, dans le cadre du sommet du Processus de Berlin <sup>(1)</sup>. Il résulte d'une démarche volontaire de la France, du Monténégro et de la Slovénie.

La lettre d'intention signée par les trois pays le 16 novembre 2022 à Podgorica, prévoyait déjà la création d'une organisation internationale, dotée d'une personnalité juridique propre. Les négociations de l'accord ont ensuite été particulièrement rapides.

### A. LES DISPOSITIONS DE L'ACCORD

L'accord comporte un préambule et vingt-quatre articles, dont la plupart sont classiques pour un accord créant une organisation internationale <sup>(2)</sup>.

Le préambule rappelle les raisons qui ont motivé la conclusion de l'accord, dont « *la multiplication des actes de malveillance dans le cyberspace qui constitue aujourd'hui l'une des principales menaces pesant sur l'environnement de sécurité régionale* ».

Le C3BO est présenté comme 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* ».

#### 1. Le statut et les missions du C3BO

L'article 1<sup>er</sup> définit dix termes de l'accord. Il distingue notamment les « membres fondateurs » que sont la France, le Monténégro et la Slovénie, des autres membres. Ces derniers peuvent être des pays ou des organisations régionales ou internationales. Ils peuvent appartenir au groupe des Balkans occidentaux, ou non.

L'article 2 précise les modalités de création ainsi que le statut juridique du C3BO : celui-ci est une « *organisation internationale et intergouvernementale en vertu du droit international* ». Il jouit à ce titre de la personnalité juridique internationale.

---

(1) Le Processus de Berlin est une initiative diplomatique lancée par l'Allemagne en 2014 pour soutenir l'intégration européenne des pays des Balkans occidentaux.

(2) L'accord se démarque surtout par les précisions sur les États pouvant être candidats, liées à la complexité de la région. De plus, les articles 15 et 16 sur le traitement des données et l'habilitation de sécurité sont originaux pour ce type d'accord mais s'expliquent par la nature même de l'organisation.



L’**article 3** fixe le siège du C3BO à Podgorica, la capitale du Monténégro, dans des conditions définies par un accord de siège <sup>(1)</sup>.

En juin 2024, le Monténégro a livré les locaux définitifs, à l’occasion d’une conférence régionale organisée par le centre. Ces locaux sont intégrés au nouveau parc scientifique et technologique de la ville. Selon le MEAE, ces locaux sont modernes, spacieux et bien équipés <sup>(2)</sup>.

L’**article 4** présente l’objectif du C3BO – la cyberrésilience de la zone – et détaille ses activités : l’organisation de formations, la mise en commun d’expériences et de bonnes pratiques et le soutien à l’élaboration d’une maquette de cours dans la sphère universitaire et régionale. L’article insiste sur son rôle dans la coopération régionale et internationale.

Parmi les personnels formés figurent des magistrats, des militaires et des membres des forces de l’ordre.

## 2. Les membres

L’**article 5** rappelle la liste des membres fondateurs du C3BO et précise qu’ils « *fournissent le capital de départ nécessaire au fonctionnement du C3BO ainsi qu’une contribution annuelle conformément à l’article 13* ». Or, pour la France, ces contributions représentent des montants élevés (cf. *infra*).

Les membres fondateurs bénéficient chacun de deux représentants au conseil d’administration.

L’**article 6** porte sur les autres membres appartenant au groupe des six pays des Balkans occidentaux. Ces États peuvent devenir membre du C3BO en adhérant à l’accord du 16 octobre 2023. Ils disposeront alors d’un représentant au conseil d’administration mais devront s’acquitter d’une contribution annuelle fixée par ce conseil pour ne pas s’exposer à une suspension de leur droit de vote.

De même, l’**article 7** prévoit l’adhésion d’autres membres, soumis à ce droit et à cette obligation : il s’agit de pays tiers ou d’organisations internationales dont la candidature serait approuvée par un vote à la majorité des deux tiers du conseil d’administration.

---

(1) Le projet d’accord de siège qui sera signé entre le C3BO et le Monténégro, a été validé par la direction des affaires juridiques du ministère des affaires étrangères du Monténégro et est en cours d’analyse au ministère des affaires étrangères de la Slovaquie. Il devra ensuite être validé par la direction des affaires juridiques du ministère de l’Europe et des affaires étrangères de la République française avant de pouvoir être finalisé et présenté au conseil d’administration du C3BO. Ce dernier se réunira dans un délai d’un mois à compter de l’entrée en vigueur de l’accord du 16 octobre 2023.

(2) Le C3BO dispose de sept salles dont trois sont équipées de plateaux techniques performants permettant d’assurer des formations. Le centre a également l’usage de deux grandes salles de conférences qui sont utilisées pour les forums, ateliers et conférences que le centre organise en partenariat avec des agences et institutions nationales, régionales ou internationales, des fondations ou des organisations non gouvernementales.

La suspension des droits de vote d'un membre peut survenir en cas de non-paiement de la contribution annuelle ou en cas de grave manquement aux objectifs communs de cybersécurité et de stabilité du C3BO (**article 8**). Elle est décidée par un vote du conseil d'administration à la majorité des trois-quarts, selon une procédure déterminée par le règlement intérieur.

En mars 2025, une délégation franco-slovène s'est rendue en Albanie, au Kosovo et en Macédoine du Nord pour présenter un projet de lettre d'intention visant à confirmer la volonté politique de ces pays de rejoindre l'organisation internationale. Les trois pays ont salué l'action du centre et le Kosovo et l'Albanie ont annoncé qu'ils pourraient le rejoindre comme membre.

### 3. L'organisation et le fonctionnement

Les articles 9 à 11 définissent la structure et la gouvernance du C3BO.

Selon l'**article 9**, le centre est composé d'un conseil d'administration, d'un conseil consultatif et d'un secrétariat. Un nouvel organe subsidiaire peut être créé par le conseil d'administration.

L'**article 10** précise le fonctionnement et le rôle du conseil d'administration. Chaque représentant dispose d'une voix et peut se faire remplacer par un suppléant. Les décisions du conseil d'administration sont prises à la majorité simple en principe, sauf pour le règlement intérieur, pour l'admission de nouveaux membres ou pour approuver des amendements à l'accord du 16 octobre 2023 : la majorité des deux-tiers est alors requise. Les missions du conseil d'administration portent principalement sur la supervision des activités du centre, la définition des programmes de travail, l'adoption du budget annuel, les nominations <sup>(1)</sup>, l'adoption du règlement intérieur et l'approbation d'accords internationaux.

L'**article 11** porte sur le conseil consultatif. Chaque membre du C3BO peut y disposer d'un représentant et des membres supplémentaires peuvent l'intégrer par un vote du conseil d'administration à la majorité simple. Le conseil consultatif élabore un programme de travail ainsi qu'un plan pluriannuel de développement du programme.

L'**article 12** détermine le mode de nomination et les attributions du directeur général en tant que représentant légal du centre. Le directeur du centre est actuellement le Français Gilles Schwoerer.

L'**article 13** prévoit la responsabilité financière des membres : ceux-ci sont « *responsables conjointement et solidairement de la prise en charge des coûts fixes du C3BO* ». De plus, il précise que c'est le conseil d'administration qui détermine le montant des contributions annuelles dues par les membres. Sur ce

---

(1) Le conseil d'administration nomme le directeur général, le directeur du programme, le commissaire aux comptes et les membres du conseil consultatif.

point, le ministère a déclaré à la rapporteure qu’il veillerait à ce que la contribution demandée à la France ne diffère pas de celle que celle-ci souhaiterait consacrer.

L’article évoque également la possibilité pour des partenaires ou des bailleurs de fonds de participer <sup>(1)</sup>.

L’**article 14** porte sur le règlement intérieur. Celui-ci est adopté à la majorité des deux-tiers lors de la première session du conseil d’administration et peut être complété par des règlements internes supplémentaires. Il précise notamment les règles relatives à la protection des données applicables au C3BO, en conformité avec les obligations internationales et, le cas échéant, européennes des parties (**article 15**).

L’**article 16** prévoit une procédure d’habilitation de sécurité pour les candidats recrutés au sein du C3BO. Cette procédure est conduite par les membres fondateurs.

#### **4. Les clauses finales**

Les **articles 17 à 22** portent sur les modalités d’entrée en vigueur, d’amendement et de dénonciation de l’accord.

L’accord entrera en vigueur le trentième jour après le dépôt du dernier instrument de ratification ou d’approbation auprès de l’État dépositaire par les membres fondateurs. La Slovénie et le Monténégro ayant terminé cette procédure <sup>(2)</sup>, l’approbation de l’accord par la France permettrait donc sa mise en œuvre.

L’**article 23** prévoit une procédure de règlement des différends.

L’**article 24** désigne le Monténégro comme dépositaire de l’accord. Après l’entrée en vigueur du texte, il en assurera l’enregistrement auprès du secrétariat des Nations unies, conformément à l’article 102 de la Charte de ces dernières.

### **B. UN TEXTE UTILE MAIS QUI NE PERMET PAS ENCORE DE RÉDUIRE L’ENGAGEMENT FINANCIER DE LA FRANCE**

#### **1. Le statut d’organisation internationale renforce et légitime le centre**

Selon le MEAE, le statut d’organisation internationale donne au C3BO « *une assise juridique solide* » et en conséquence, « *une réelle sécurité juridique dans un environnement régional complexe* ». Plus spécifiquement, il lui permet de bénéficier d’une personnalité juridique internationale.

---

(1) *Quel que soit l’acteur, les contributions peuvent être financières ou en nature.*

(2) *La Slovénie a procédé à la ratification le 14 août 2024. Le président du Monténégro Jakov Milatovic a signé l’instrument de ratification le 10 mars 2025 après que le Parlement a ratifié l’accord (loi sur la ratification publiée au Journal officiel du Monténégro daté du 19 février 2025).*

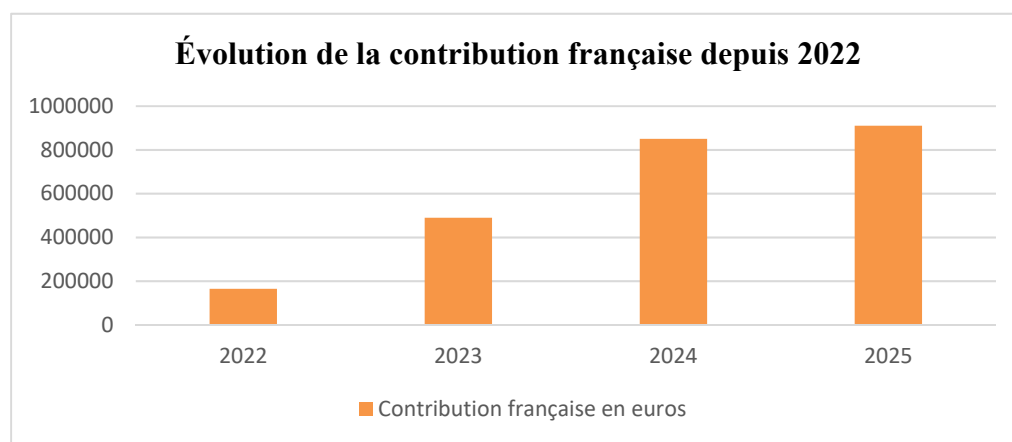
De plus, la gouvernance est précisée et le principe d'une contribution financière des membres se trouve acté.

Ce statut permet également au C3BO de disposer d'une légitimité suffisante pour entretenir des relations avec d'autres acteurs internationaux, tels que les organisations internationales ou des organisations non gouvernementales, et surtout d'accueillir en son sein d'autres États – de la région ou en dehors – et des organisations internationales. Ainsi, ce statut faciliterait la recherche de partenariats et l'intégration de nouveaux membres, et donc *in fine*, de financements <sup>(1)</sup>.

Enfin, il déchargerait l'ambassade de France au Monténégro de la gestion comptable directe de la contribution française à ce centre, qui représente une charge de travail importante pour cette petite ambassade.

## 2. Une contribution financière française trop élevée

Le graphique ci-dessous présente la contribution de la France au C3BO depuis 2022. Celle-ci n'a cessé d'augmenter pour suivre l'augmentation des formations proposées. Elle atteindra 910 000 euros en 2025 (dont 460 000 euros de dépenses de personnel (titre 2) ; contre 850 000 euros en 2024), à mettre en regard de la contribution de 200 000 euros de la Slovénie (100 000 euros en 2024). Le Monténégro, pour sa part, loue le site pour environ 80 000 euros par an.



Dans un contexte de contraintes budgétaires fortes pour les dépenses publiques nationales, la rapporteure recommande de réduire cette subvention française au C3BO à l'avenir. Le MEAE lui-même évoque un objectif de « rééquilibrage des contributions ».

Or la Commission européenne a récemment acté le principe d'une subvention de 3,5 millions d'euros de l'Union européenne sur la période 2025-2027. La rapporteure espère que la contribution française sera réduite en conséquence.

---

(1) À court terme, la transformation en organisation internationale devrait néanmoins contribuer à une augmentation de la masse salariale, difficilement quantifiable à ce stade.

## EXAMEN EN COMMISSION

*Le mercredi 7 mai 2025, à 11 heures, la commission examine le projet de loi, adopté par le Sénat, autorisant l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO).*

**Mme Laetitia Saint-Paul, présidente.** Mes chers collègues, notre ordre du jour appelle l'examen du projet de loi, adopté par le Sénat, autorisant l'approbation de l'accord portant création du centre de développement des capacités cyber dans les Balkans occidentaux (C3BO).

La cybersécurité constitue dorénavant un enjeu majeur de l'environnement numérique mondial. Face à des attaques de plus en plus sophistiquées et agressives, certains États peuvent se trouver ébranlés, tels le Monténégro et l'Albanie en 2022. Les pays des Balkans occidentaux constituent des cibles faciles pour des entreprises d'ingérence étrangère, tout particulièrement de la Russie, en raison de l'insuffisance de leurs moyens en matière de cybersécurité. De ce fait, ils représentent un risque de compromission par rebond de notre propre cyberspace, national et européen.

L'accord relatif à la création d'un centre de développement des capacités cyber dans les Balkans occidentaux conclu à Tirana le 16 octobre 2023 entre la France, le Monténégro et la République de Slovénie, dont il nous est demandé d'autoriser l'approbation, est une initiative particulièrement opportune. Ce centre, implanté à Podgorica, dispensera trente-et-une formations par an sur la cybersécurité, au bénéfice de quelque 600 personnels des États de la région, pour un coût global de 1,05 million d'euros, assumé à 83 % par notre pays.

Ce nouvel organisme est porteur d'un signal fort ; il renforcera le partenariat liant la France à cette région d'importance géostratégique majeure. Il me semble donc opportun que nous adoptions ce projet de loi, comme l'a fait le Sénat le 12 février dernier.

**Mme Marine Hamelet, rapporteure.** L'accord sur le C3BO a été signé le 16 octobre 2023 à Tirana par les représentants de la France, du Monténégro et de la Slovénie. Il ne faut pas se fier au titre de l'accord, qui vise en réalité à transformer le C3BO en organisation internationale. Ce centre fonctionne depuis 2022 et a formé, à ce jour, plus de 400 personnes. Ce texte offre à notre commission l'occasion d'évoquer la situation dans les Balkans occidentaux et notre cyberdiplomatie, dont le C3BO est un exemple original.

Les Balkans occidentaux sont composés de six pays : l'Albanie, la Bosnie-Herzégovine, le Kosovo, la Macédoine du Nord, le Monténégro et la Serbie. La région rassemble, sur une superficie légèrement inférieure à celle du

Royaume-Uni, 17 millions d'habitants. Plus de trente ans après l'éclatement de la Yougoslavie, elle demeure marquée par de fortes tensions et par des défis institutionnels et sécuritaires majeurs.

Sous la législature précédente, j'ai eu l'occasion, avec notre collègue Frédéric Petit, de présenter devant cette commission un rapport d'information issu d'un déplacement en Bosnie-Herzégovine, en Serbie et en Albanie, effectué en mars 2023. Les défis que nous avons identifiés semblent malheureusement toujours d'actualité : consolidation de la démocratie et de l'État de droit ; maîtrise des risques sécuritaires ; transition énergétique ; recul démographique ; persistance de foyers de crise internes potentiellement déstabilisateurs. Dans mon rapport sur ce projet de loi, je présente des exemples récents de ces nombreux défis sécuritaires.

La région est confrontée à de nombreux trafics : êtres humains, armes, stupéfiants, véhicules. Les relations bilatérales entre certains États de la zone peuvent susciter de fortes tensions. Frédéric Petit, Pierre Pribetich, Jean-Louis Roumégas et moi-même menons actuellement une mission visant à apporter une contribution parlementaire à la définition des contours d'un accord de paix entre la Serbie et le Kosovo. Nous devrions publier notre rapport à l'automne.

La plupart de ces pays sont très vulnérables à la cybercriminalité. L'Albanie et le Monténégro ont subi des attaques à l'été 2022. À cette occasion, des infrastructures gouvernementales ont été la cible de cyberattaques majeures. Pour l'Albanie, l'attaque viendrait d'Iran ; pour le Monténégro, de la Russie.

Ces attaques s'inscrivent dans le cadre de la guerre dite « hybride ». Ces pays manquent de personnel qualifié pour y faire face, voire sont devenus dépendants de compétences étrangères. Tel est le cas du Monténégro, qui a confié une grande partie de sa cybersécurité à des experts américains, dont les contrats ont été résiliés après l'élection de Donald Trump.

Pour améliorer leur cybersécurité, certains pays modifient leur cadre réglementaire et institutionnel. Tel est le cas de la Serbie et, dans une moindre mesure, de l'Albanie et, progressivement, du Monténégro. Tel n'est pas encore le cas de la Bosnie-Herzégovine.

S'agissant des conséquences de cette cybervulnérabilité pour la France, elle pourrait, d'après le ministère de l'Europe et des affaires étrangères (MEAE), encourager les cyberattaques menées depuis les Balkans et les opérations menées contre des réseaux communs, notamment ceux de l'Organisation du traité de l'Atlantique Nord (OTAN). En outre, l'espace cyber est utilisé par d'autres criminels, notamment les narcotrafiquants, que j'évoque dans mon rapport. Limiter le développement de la cybercriminalité dans les Balkans occidentaux permettrait de lutter contre d'autres formes de criminalité dans la région ou peut-être sur le sol français.

J'en viens au C3BO : créé le 16 novembre 2022 par un mémorandum signé par la France, le Monténégro et la Slovénie, il est situé à Podgorica, capitale du

Monténégro. Il organise des événements et des formations dans trois domaines : la lutte contre la cybercriminalité, la cybersécurité et la cyberdiplomatie. Il a réalisé cinq formations en 2023, vingt-et-une en 2024 pour 400 stagiaires et prévoit d'en organiser trente-cinq en 2025 pour 600 stagiaires.

Les stagiaires accueillis sont originaires d'Albanie, de Bosnie-Herzégovine, du Kosovo, de Macédoine du Nord, du Monténégro, de Serbie et de Moldavie. La France déploie trois expatriés sur place ; la Slovénie rémunère les trois employés locaux et enverra prochainement une diplomate. Des acteurs du cyber, français pour la plupart, contribuent ponctuellement aux formations, selon les besoins.

J'en viens au cadre dans lequel s'inscrit le projet. Paradoxalement, la cybersécurité a été inscrite tardivement dans la stratégie interministérielle pour les Balkans occidentaux. Elle ne figure pas dans sa version initiale, publiée en 2019, et a été insérée en 2023.

Le C3BO relève avant tout d'une initiative de cyberdiplomatie, théorisée progressivement par plusieurs textes : la stratégie internationale de la France pour le numérique, publiée en 2017 ; la revue stratégique de cyberdéfense, publiée en 2018 ; la revue nationale stratégique (RNS) de 2022. La cyberdiplomatie vise à renforcer la coopération dans le domaine cyber avec les pays partenaires, par exemple pour lutter ensemble contre la cybercriminalité et échanger des renseignements, et la coopération bilatérale en général.

Pour le groupe Rassemblement national, le C3BO ne doit pas être compris comme une étape favorisant l'élargissement de l'Union européenne (UE) aux pays des Balkans occidentaux en leur permettant de s'aligner sur le droit européen. Au demeurant, cette position est celle du pouvoir exécutif français. Pour nous, le C3BO doit être considéré uniquement comme une occasion d'approfondir des relations bilatérales dans la région s'agissant d'un domaine stratégique. Nous défendons une approche bilatérale.

L'accord du 16 octobre 2023 est composé de vingt-quatre articles de facture classique, que je détaille dans le rapport. Il vise à transformer le C3BO en organisation internationale. Ce statut lui accorde la personnalité juridique internationale et renforce sa légitimité ainsi que son attractivité. À l'heure actuelle, il ne compte – c'est à mes yeux sa faiblesse – que ses trois membres fondateurs : la France, la Slovénie et le Monténégro.

L'accord permet à d'autres pays européens, notamment ceux des Balkans occidentaux, et à des organisations internationales de rejoindre le C3BO. Les nouveaux membres devront s'engager à participer à son financement, en échange notamment d'un siège au conseil d'administration, où chaque membre fondateur dispose de deux sièges.

Si cet accord semble utile pour renforcer le C3BO et attirer de nouveaux membres, il ne règle pas la question, essentielle pour le groupe Rassemblement national, de la contribution financière trop élevée de la France. En 2025, notre pays

dépensera près de 1 million d'euros pour financer le C3BO, alors même que nos finances publiques sont très contraintes.

Nous recommandons, comme l'a fait le Sénat lorsqu'il a examiné le texte en février, de réduire nettement la subvention française. Dès lors que le MEAE ne s'y est pas engagé et que la perspective d'intégration des pays des Balkans occidentaux à l'Union européenne est défendue par la France, le groupe Rassemblement national s'opposera au texte.

**Mme Laetitia Saint-Paul, présidente.** Nous en venons aux interventions des orateurs des groupes politiques.

**Mme Liliana Tanguy (EPR).** Je salue l'excellence des relations diplomatiques entre la France et le Monténégro, dont les échanges se sont intensifiés au cours des dernières années, dans un climat de confiance et de coopération. Le Monténégro est un partenaire fiable, résolument engagé sur la voie de l'Union européenne et dont les progrès dans la mise en œuvre des réformes sont reconnus, notamment en matière de lutte contre la corruption et de consolidation de l'État de droit.

Je suis personnellement impliquée de longue date dans ce domaine, notamment en tant que vice-présidente de la sous-commission sur les Balkans, chargée d'un rapport sur le dialogue post-suivi avec le Monténégro par l'Assemblée parlementaire du Conseil de l'Europe (APCE). Dans cette fonction, j'ai pu constater concrètement les avancées du pays dans le cheminement vers l'adhésion à l'Union européenne.

Dans ce contexte, je souhaite souligner l'importance stratégique du C3BO. Promu par la France, la Slovénie et le Monténégro, il incarne une initiative pionnière visant à renforcer la cybersécurité et la stabilité régionales, qui sont deux enjeux indissociables. Le choix de Podgorica pour accueillir ce centre, que j'ai eu l'occasion de visiter en mars aux côtés du ministre délégué chargé de l'Europe, Benjamin Haddad, est tout sauf symbolique.

Le Monténégro est le pays des Balkans occidentaux le plus avancé sur la voie de l'intégration européenne. Il est très engagé dans la coopération avec la France. Le C3BO s'inscrit donc pleinement dans la volonté exprimée par le président de la République d'élaborer une stratégie française cohérente et ambitieuse pour les Balkans occidentaux.

Le groupe Ensemble pour la République soutient pleinement le projet de loi autorisant l'approbation de l'accord fondateur du C3BO et lui attribuant le statut d'organisation internationale. L'ambition est de faire du C3BO un véritable pôle régional de formation, de coopération opérationnelle et de montée en compétences, mais aussi de convergence réglementaire avec les standards européens, notamment par la mise en œuvre de la directive concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (NIS 2).



Par ailleurs, il s'agit d'un investissement stratégique renforçant le rôle de puissance cyber de la France. Son coût, rapporté au coût humain, politique et économique d'une attaque de grande ampleur ou d'une instabilité régionale mal contenue, est faible. Le C3BO est un outil concret méritant d'être élargi à d'autres pays des Balkans occidentaux, dans une logique de solidarité et de sécurité partagée avec une région faisant l'objet d'influences étrangères hostiles, afin de protéger nos démocraties et d'assurer la sécurité collective de l'Europe.

**Mme Marine Hamelet, rapporteure.** Nous sommes au moins d'accord sur un point : le Monténégro est le pays des Balkans occidentaux ayant consenti le plus d'efforts pour se rapprocher de l'Union européenne, avec laquelle trente-trois chapitres ont été ouverts à la négociation, dont six clôturés à titre provisoire. Cette observation sert mon argumentation selon laquelle ce projet de loi est surtout un prétexte pour favoriser l'adhésion des pays concernés à l'Union européenne, davantage qu'un moyen de résoudre un problème de cybercriminalité ou de cyberdiplomatie. Sur ce point, nous avons une divergence.

Quant à son coût, il n'est pas faible à mes yeux. L'argent public français doit être surveillé et ne peut servir à faire n'importe quoi. Un million d'euros, ce n'est pas rien. En matière budgétaire, les Français souhaitent savoir où va leur argent et entendent qu'il soit dépensé à bon escient.

**Mme Liliana Tanguy (EPR).** La sécurité est elle-aussi importante pour les Français !

**M. Arnaud Le Gall (LFI-NFP).** Je ne suis pas d'accord avec les considérations strictement budgétaires mises en avant par la rapporteure. Compte tenu de l'effet de levier escompté, 1 million d'euros, ce n'est rien. Il est fondamental que la France coopère avec d'autres pays en matière de sécurité numérique, au bénéfice du transfert d'expertise et de l'influence, et d'autant plus que les enjeux sont communs.

Si je suis dubitatif sur le projet de loi, c'est parce qu'il procède de l'idée d'adapter et de préparer les pays concernés à une éventuelle entrée dans l'Union européenne. En la matière, notre position est très claire : pas d'élargissement sans consolidation, sans davantage de démocratie et sans harmonisation, sociale et fiscale notamment.

Par ailleurs, les règlements européens en matière numérique sont très contestables. S'ils affichent de grandes ambitions, leurs réalisations sont maigres. C'est à juste titre que notre collègue Latombe mène devant la Cour de justice de l'Union européenne (CJUE) un combat, hélas solitaire, sans même l'aide de nos administrations, pour faire annuler l'accord de transfert des données entre l'Europe et les États-Unis, qui enfreint le règlement général sur la protection des données (RGPD). Il soulève un problème de fond : il y a des failles partout. Cet accord ne nous protège aucunement du pillage des données personnelles, notamment par les

GAFAM – Google, Apple, Facebook, Amazon et Microsoft. Que valent les grandes ambitions sans moyens pour les réaliser ?

Quant à notre souveraineté et à notre autonomie, elles dépendent notamment des infrastructures matérielles. La France a un vrai savoir-faire, notamment en matière de lutte contre les cyberattaques, comme l’a montré l’audition ce matin du directeur général de l’Agence nationale de la sécurité des systèmes d’information (ANSSI).

Que nous coopérons avec d’autres pays, notamment ceux concernés par l’accord qu’il nous est demandé de ratifier, est une bonne chose. Mais il n’est pas vrai que nous puissions fournir des solutions couvrant tout le spectre cyber sans investir réellement dans les moyens nationaux. Telle n’est pas la politique que nous menons, qui prétend, de façon parfaitement contradictoire, construire une souveraineté nationale en s’appuyant sur les GAFAM.

Nous nous abstiendrons donc sur ce texte.

**Mme Marine Hamelet, rapporteure.** Nous avons un point de convergence : non à l’élargissement.

S’agissant des considérations financières, le problème est que l’accord n’offre aucun cadre. Notre contribution est passée de 165 000 euros en 2022 à 910 000 euros en 2025. Compte tenu de la taille du C3BO et de l’augmentation prévue du nombre de formations dispensées, rien n’exclut que nos dépenses augmentent significativement, d’autant que les coûts relatifs aux bénéficiaires sont intégralement pris en charge. Nous souhaitons que la répartition de la dépense soit améliorée. La France contribue au C3BO à hauteur de 80 % : à nos yeux, ce n’est pas normal.

**M. Alain David (SOC).** Figurant parmi les grandes orientations en matière de sécurité énoncées en 2022 dans la Boussole stratégique européenne, le cyberspace est devenu un domaine de concurrence stratégique, dans une période de dépendance croissante à l’égard des technologies numériques. La cybersécurité constitue dorénavant un enjeu majeur de l’environnement numérique mondial, caractérisé par la montée en puissance fulgurante, qualitative et quantitative, des capacités d’agression, parfois avec le concours de l’intelligence artificielle (IA), comme l’attestent les travaux que nous menons au sein de notre commission.

Les pays des Balkans occidentaux sont pris dans un jeu d’influence et d’ingérence très agressif mené notamment par la Russie et par la Chine. En août 2022, le Monténégro a été confronté à une attaque cyber d’ampleur, incluant des ingérences électorales directes. À cette occasion, l’ANSSI a été dépêchée sur place, dans le cadre de sa première intervention internationale.

L’Union européenne, suivie par la France en 2019, a adopté sa stratégie s’agissant des Balkans occidentaux, où se joue une compétition d’influence. L’avancement du processus d’adhésion à l’Union européenne de ces pays,

laborieusement entamé, est, à des degrés divers, contrarié par une succession de blocages. Or l’Albanie en 2009, le Monténégro en 2017 et la Macédoine en 2020 ont rejoint l’OTAN, et la Bosnie-Herzégovine est engagée dans un processus d’adhésion.

L’instauration du C3BO vise à renforcer leurs capacités en matière de lutte contre la cybercriminalité dans de multiples domaines : capacités opérationnelles des services de police et de justice ; prévention des attaques cyber ; gestion des risques ; implication des décideurs-clés dans les enjeux ; cyberdiplomatie. L’accord qui nous est soumis nourrit le partenariat entre la France et cette région d’importance géostratégique majeure. Il incarne la cyberdiplomatie menée par la France, qui cherche à se positionner comme une puissance cyber. Il permet d’approfondir la coopération entre les acteurs de la région des Balkans et d’harmoniser les normes applicables dans la perspective de leur adhésion future à l’Union européenne.

Le groupe Socialistes et apparentés soutient cet accord.

**Mme Marine Hamelet, rapporteure.** Je ne pense pas que ce projet contribuera à harmoniser les normes applicables dans cette région. Même s’ils y envoient des personnes en formation, très peu de pays sont membres du C3BO.

Assez curieusement, la principale attaque a touché l’Albanie en 2022. Or ce pays a développé un système de défense indépendant, qui n’a rien à voir avec le C3BO.

Cet accord n’aidera pas à améliorer les relations entre les États de la région. Il risque même, selon moi, de créer davantage de dissensions. Chacun développe son propre système. La Serbie, qui est très avancée dans le domaine cyber, ne coopérera pas avec le Kosovo. Le fait de s’immiscer dans ces affaires me semble assez dangereux pour les relations entre les pays de la zone de Balkans.

**Mme Catherine Hervieu (EcoS).** La stratégie interministérielle pour les Balkans occidentaux vise à stabiliser les six pays de cette zone, à favoriser leur développement économique et à renforcer l’État de droit et les droits sociaux dans la perspective de leur adhésion à l’UE.

Cette démarche a aussi son importance pour faire face à la guerre hybride sur notre continent, qui crée de nouveaux champs de conflictualité, notamment dans les espaces cyber et informationnel. Dans sa Boussole stratégique adoptée en 2022, l’UE a prévu de développer une boîte à outils hybride pour répondre à l’importance croissante de ces menaces, qui proviennent notamment de la Russie. Le renforcement de la coopération avec les pays des Balkans occidentaux constitue une étape dans leur marche vers l’intégration dans l’UE.

En matière de lutte contre les cyberattaques, la France et la Slovénie ont lancé en novembre 2022 le C3BO, installé au Monténégro. L’objectif est de

renforcer les capacités cyber des forces de police, des magistrats et des opérateurs de cybersécurité des partenaires balkaniques de l'UE. Nous soutenons sa création.

En effet, on assiste à une série de cyberattaques en Albanie et dans la région depuis juillet 2022. Elles ont commencé en Macédoine du Nord et sont semblables à celles qui ont visé l'Ukraine fin décembre 2015. Le réseau d'approvisionnement en électricité avait alors été mis hors service.

La création de ce centre est cruciale car la région est très vulnérable aux activités de désinformation menées depuis l'étranger, lesquelles se sont intensifiées ces dernières années. La Bosnie-Herzégovine, le Monténégro et la Serbie sont les pays les plus touchés par les opérations russes de désinformation visant à décrédibiliser l'UE et l'OTAN. Par effet domino, ces actions affectent aussi les pays avoisinants, donc l'espace européen.

Pourriez-vous préciser les moyens techniques et les coopérations mis en œuvre pour lutter contre la désinformation d'origine russe dans la région, afin notamment de renforcer les mécanismes de protection destinés à faire face à la manipulation des processus électoraux ?

**Mme Marine Hamelet, rapporteure.** Il est indéniable que des attaques proviennent de la Russie mais tel n'est pas le cas de toutes. J'ai donné l'exemple des attaques iraniennes contre l'Albanie. On sait qu'il s'agit de mesures de rétorsion liées au fait que celle-ci a accueilli des membres de l'Organisation des moudjahidines du peuple iranien.

Les cyberattaques viennent de toutes parts ; les centres comme le C3BO ont pour mission de les parer. La Serbie a monté le sien, très compétent, de manière indépendante. Les disparités en matière d'expertise sont d'ailleurs très fortes dans la région, de la Serbie, très au point, à la Bosnie-Herzégovine, où il n'y a quasiment rien.

**Mme Catherine Hervieu (EcoS).** D'où, justement, la nécessité d'une intégration dans l'UE !

**Mme Marine Hamelet, rapporteure.** C'est votre point de vue. Je ne le partage pas.

**Mme Maud Petit (Dem).** L'intitulé du projet de loi est quelque peu trompeur : il s'agit de valider la transformation du C3BO en organisation internationale. Il a été créé le 16 novembre 2022 par un mémorandum signé par la France, le Monténégro et la Slovaquie.

La création de ce centre s'explique par plusieurs raisons. La première est l'extrême vulnérabilité des pays des Balkans occidentaux à la cybercriminalité. Cette région est le maillon faible de la cybersécurité européenne.

En 2022, l’Albanie a subi des cyberattaques attribuées à l’Iran qui ont visé des données gouvernementales et le système informatique des douanes. Peu de temps après, le Monténégro était lui aussi victime d’une cyberattaque de grande ampleur affectant plusieurs de ses institutions. La vulnérabilité de cette région – où subsistent encore de nombreuses tensions, liées notamment à l’écclatement de la Yougoslavie et à la guerre du Kosovo – s’explique en partie par le développement rapide du numérique sans que la population ait été suffisamment sensibilisée aux enjeux. Cette vulnérabilité découle aussi des difficultés rencontrées pour recruter et fidéliser des spécialistes.

Il apparaît également que tous ces États n’ont pas encore pris la pleine mesure des dangers de la cybercriminalité. La Serbie a adopté une loi sur la cybersécurité mais d’autres pays comme le Kosovo, la Macédoine du Nord et la Bosnie-Herzégovine ne sont pas encore dotés de moyens de lutte efficaces contre ces attaques d’un nouveau genre. Si éloignée qu’elle puisse paraître, leur vulnérabilité n’est pas sans conséquence pour notre pays. L’espace cyber étant ouvert, il est nécessaire d’empêcher que la cybercriminalité qui se développe dans les Balkans gagne les autres États de l’UE.

Tel est précisément l’un des enjeux de la participation de la France au C3BO. Celui-ci est également un moyen pour notre pays d’affirmer sa présence dans une région stratégique. Le groupe Les Démocrates votera donc en faveur de ce texte.

Madame la rapporteure, par-delà votre opposition au financement par la France de ce centre et votre refus de voir s’élargir l’UE, nous aimerions savoir pourquoi vous estimez que l’implication de la France dans le C3BO ne constitue pas un moyen de préparer ces pays des Balkans à l’adhésion à l’UE. Cela les aide notamment à se rapprocher des exigences de la directive NIS 2, qui permet à des milliers d’entités de mieux se protéger.

**Mme Marine Hamelet, rapporteure.** La France n’a pas à assumer seule les dépenses destinées à aider cette région. Nous subissons aussi des attaques.

Nous disposons d’entreprises privées très pointues dans ce domaine, qui pourraient intervenir et interviendront pour faire face aux attaques, qui sont ponctuelles.

Vous avez évoqué le manque de personnel dans ces pays. On ne m’a pas fait part de ce problème. Le nombre de personnes formées ne cesse d’augmenter, ce qui montre qu’il y a une demande.

**Mme Maud Petit (Dem).** Même si la transformation du C3BO en organisation internationale ne permettra peut-être pas à la France de se désengager, elle pourrait conduire à réduire notre contribution puisque d’autres pourraient prendre le relais.

**Mme Marine Hamelet, rapporteure.** L'accord qui nous est soumis ne fournit aucune assurance en ce sens. L'étude d'impact fourmille de suppositions mais il n'y a rien de concret. Elle n'indique à aucun moment que d'autres pays participeront au financement du centre, ce qui permettrait à la France de se désengager.

**M. Michel Guiniot (RN).** Je me pose un certain nombre de questions sur le contenu de cet accord.

Le projet de ratification a été déposé au Sénat le 27 novembre 2024, alors que les locaux définitifs du C3BO avaient déjà été livrés en juin de la même année. Les premières actions de formation ont été organisées en mai 2023, soit avant la signature de l'accord signé à Tirana en octobre 2023.

Quel est notre rôle, si ce n'est faire office de chambre d'enregistrement ?

La contribution française a même été engagée par une simple lettre d'intention. Pourtant, si l'article 52 de la Constitution précise que le président de la République négocie et ratifie les traités, les traités ou accords relatifs à l'organisation internationale ne peuvent être ratifiés ou approuvés qu'en vertu d'une loi. L'article 53 est très clair : ils ne prennent effet qu'après avoir été ratifiés ou approuvés. Comment se fait-il que cet accord produise déjà des effets et que le Parlement soit traité comme une chambre d'enregistrement ? Cette question a été posée au Sénat sans qu'une réponse y soit apportée.

La France assure plus de 80 % du financement de ce projet, qui s'intègre dans la stratégie interministérielle pour les Balkans occidentaux. Le ministère a-t-il précisé quelle sera la langue de travail dans ce centre ?

Votre rapport, celui du Sénat et l'étude d'impact soulignent que les contributions des États à ce projet sont déséquilibrées. Le Monténégro, où le salaire minimum s'élève à 670 euros, paie 80 000 euros pour le bail du site. La Slovénie verse 200 000 euros pour rémunérer trois employés locaux et un expert. Nous payons tout le reste.

Pourtant, selon l'article 13 de l'accord, les États signataires sont responsables conjointement et solidairement de la prise en charge des coûts fixes du C3BO. De plus, une contribution annuelle sera fixée pour tous les pays par le nouveau conseil d'administration, sous réserve qu'ils s'y soumettent.

Madame la rapporteure, comme l'article 17 interdit aux signataires d'émettre toute forme de réserve, le MEAE vous a-t-il confirmé que les autres pays sont prêts à revoir les modalités de financement de ce centre qui, en devenant une organisation internationale, aura certainement des coûts accrus ?

Puisque la France paie déjà pour cet organisme, l'accord du Parlement n'est pas indispensable, surtout si l'on considère la manière dont sont répartis les coûts et

le contexte économique actuel. Je suis tout à fait conscient qu'il s'agit d'un sujet important mais le projet nous est présenté de façon assez déloyale.

**Mme Marine Hamelet, rapporteure.** Nous n'avons aucune garantie que d'autres pays participeront à ce centre. Le Monténégro a été choisi parce qu'il entretient de bonnes relations avec les autres États des Balkans. Cela a permis de les inciter à rejoindre le projet, sans assurance sur ce point jusqu'à présent.

L'accord ne prévoit pas de créer le C3BO mais de le transformer en organisation internationale. Il est donc normal que le centre ait commencé à fonctionner.

Le Sénat s'est interrogé sur la langue de travail du centre. Après l'examen du texte, le sénateur Mickaël Vallet a posé une question écrite à ce sujet, restée sans réponse à ce jour. L'accord est rédigé en français et en anglais. Il est probable que les deux langues seront utilisées, l'anglais davantage que le français dans la mesure où cette langue domine dans le domaine cyber.

**Mme Laetitia Saint-Paul, présidente.** Je m'exprimerai ici au nom du groupe Horizons. Nous venons d'auditionner le directeur de l'ANSSI. Il nous a rappelé que la France peut subir des dommages collatéraux et à quel point la vulnérabilité de nos partenaires peut nous affecter.

Face au risque élevé d'attaques par capillarité, investir 1 million d'euros dans ce centre me paraît judicieux. Quel que soit le champ de conflictualité, notre sécurité commence bien au-delà de nos frontières. Il importe d'en avoir pleinement conscience.

Nous approuvons pour notre part le projet de loi.

**Mme Marine Hamelet, rapporteure.** Vous parlez des risques par capillarité mais les pays les plus touchés, comme l'Albanie, ne sont pas membres de ce centre. J'y vois un obstacle.

Les moyens dont disposent les pays de cette région sont très inégaux. En outre, ils ne s'entendent pas entre eux. Lorsque nous nous sommes rendus au Kosovo le mois dernier, nous avons constaté que la communication était impossible entre certains États des Balkans. Tant qu'il n'y aura pas davantage de cohésion entre eux, l'efficacité de ce centre sera très réduite.

**Mme Laetitia Saint-Paul, présidente.** J'ai espoir que ce type d'initiative permette d'améliorer l'entente entre pays de la région.

Nous en venons aux interventions et questions formulées à titre individuel.

**Mme Constance Le Grip (EPR).** Je soutiens le projet de loi visant à doter le C3BO du statut d'organisation internationale.

Il ne faut absolument pas sous-estimer les dangers qui sont aux frontières de l'UE et menacent notre cybersécurité ainsi que notre capacité à résister ensemble aux cyberattaques de toute nature ; elles sont légion. Ce sont la sécurité et la stabilité du continent européen qui seront à court, moyen et long termes renforcées grâce à la coopération en matière de cybersécurité que le C3BO à vocation à inscrire dans la durée.

Par ailleurs, nous sommes capables d'exercer et de faire reconnaître un leadership réel. Nous avons la chance de pouvoir nous appuyer sur l'ANSSI et sur le service de vigilance et de protection contre les ingérences numériques étrangères (Viginum). Nous disposons d'agences et de professionnels à l'expertise excellente. Il faut en être fier et les faire rayonner au sein de structures comme le C3BO.

Compte tenu de l'importance des attaques et des ingérences numériques étrangères qui viennent de partout, notamment de Russie – France Diplomatie a dénoncé hier les cyberattaques en provenance du territoire russe utilisant le mode opératoire Storm-1516 –, il faut soutenir le changement de statut qui nous est proposé.

**Mme Marine Hamelet, rapporteure.** Je ne conteste pas nos capacités ni notre expertise, notamment celle d'entreprises privées, mais je n'en déduis pas que nous devons coopérer au C3BO. On peut très bien agir dans un autre cadre.

Je ne sous-estime pas non plus les dangers. Je pense même que le simple fait que des pays des Balkans occidentaux souhaitent entrer dans l'UE représente un danger pour eux. Des pays très puissants – pas seulement la Russie – pourraient les attaquer davantage pour bloquer le processus.

**Mme Liliana Tanguy (EPR).** Le projet de loi vise à changer le statut d'un centre qui existe déjà. Il ne s'agit donc pas, pour la rapporteure, de parler de l'élargissement de l'UE ou de donner son avis sur l'adhésion du Monténégro ou d'un autre pays des Balkans occidentaux. Ce processus est en cours.

Le texte vise avant tout à renforcer la résilience collective de l'Europe, donc de la France, dans le domaine cyber. Si vous êtes patriote, il faut soutenir ce centre créé à l'initiative de la France et de la Slovénie. Cela a en effet un coût mais il est très faible par rapport aux conséquences d'une cyberattaque à grande échelle ou d'une instabilité dans la région.

La France a tout à fait raison de soutenir ce centre, qui est amené à se développer. Pour m'y être rendue, je peux témoigner que d'autres pays souhaitent y participer. Le groupe Rassemblement national fait donc un mauvais calcul en s'opposant au projet de loi.

**Mme Marine Hamelet, rapporteure.** Certains pays sont peut-être enclins à participer mais ils ne l'ont pas encore fait alors que le centre a été créé en 2022.



**Mme Liliana Tanguy (EPR).** Ce n'est pas une raison pour renoncer à changer le statut du C3BO.

**Mme Marine Hamelet, rapporteure.** Vous me reprochez de parler de leur marche vers l'adhésion à l'UE. L'étude d'impact précise que les pays des Balkans occidentaux sont « *dans ce contexte une priorité française, notamment dans le cadre de la Communauté politique européenne et de l'intégration européenne* ». Ce n'est donc pas un fantasme : c'est écrit noir sur blanc.

\*

**Article unique** (autorisation de l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux, fait à Tirana le 16 octobre 2023)

*La commission **adopte** l'article unique **non modifié**.*

*L'ensemble du projet de loi est **ainsi adopté**.*



**ANNEXE 1 :  
TEXTE DE LA COMMISSION DES AFFAIRES ÉTRANGÈRES**

**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.



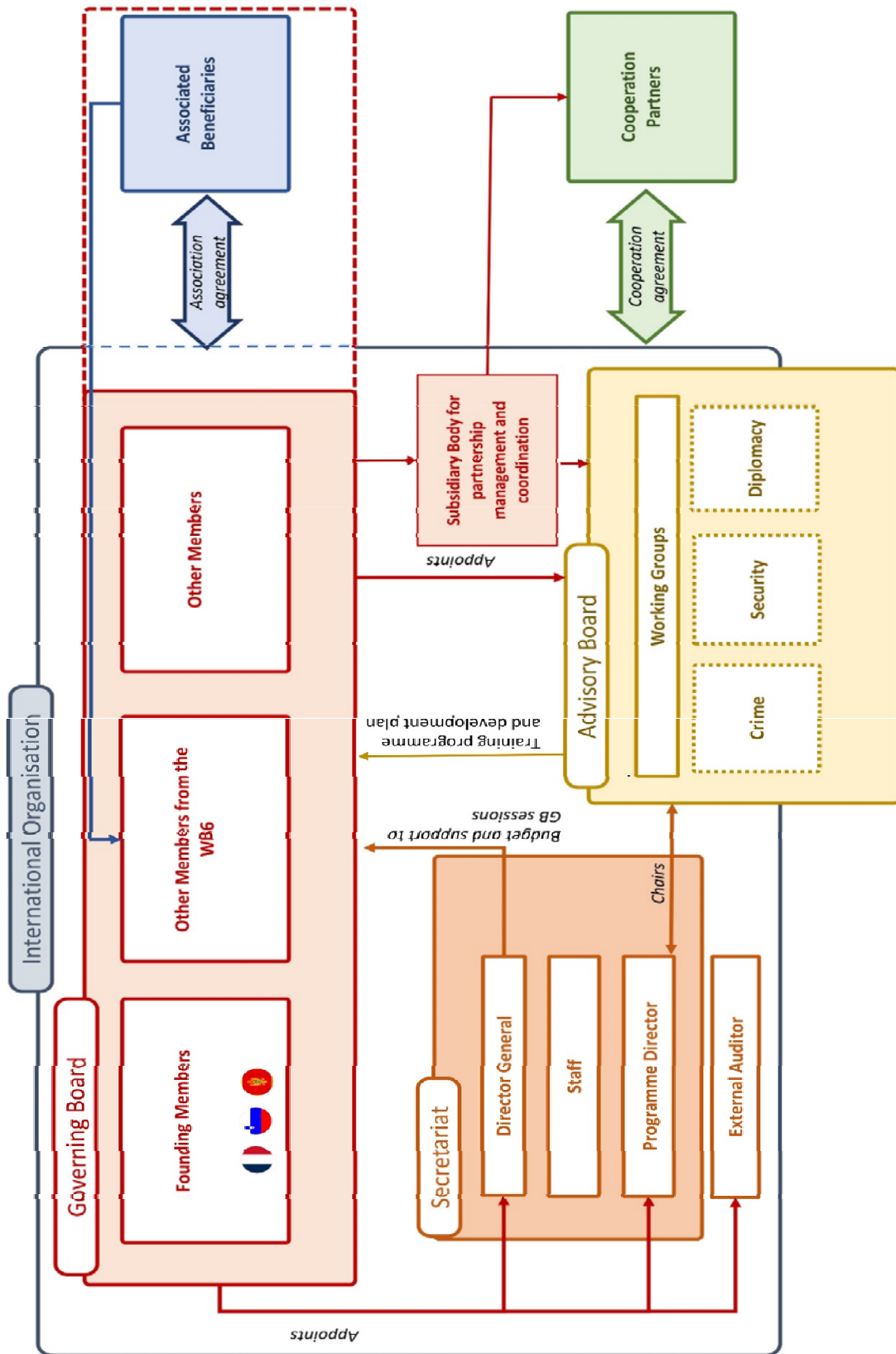
## **ANNEXE 2 : LISTE DES PERSONNES AUDITIONNÉES PAR LA RAPPORTEURE**

### **Ministère de l'Europe et des affaires étrangères**

- **Mme Anne-Marie Maskay**, ambassadrice de France au Monténégro ;
- **M. Léonard Rolland**, sous-directeur de la cybersécurité ;
- **M. Mahé Dersoir**, rédacteur, sous-direction de la cybersécurité ;
- **M. Guillaume Narjollet**, adjoint du sous-directeur des questions multilatérales et sectorielles ;
- **Mme Marguerite Costa de Beauregard**, sous-directrice de l'Europe balkanique ;
- **Mme Gabrielle Jouve**, rédactrice Monténégro et questions relatives à la sécurité dans les Balkans, sous-direction de l'Europe balkanique ;
- **Mme Aude-Line Ferrand**, adjointe au chef de la mission de l'Allemagne et de l'Europe alpine et adriatique ;
- **M. Corentin Santilli**, rédacteur, mission de l'Allemagne et de l'Europe alpine et adriatique ;
- **M. Pierre Dousset**, conseiller juridique à la mission des accords et traités, direction des affaires juridiques.



## ANNEXE 3 : FUTURE ORGANISATION DU C3BO



Source : page « Organisation » du site Internet du C3BO (consulté le 2 mai 2025).





## **ANNEXE 4 : STRATÉGIE FRANÇAISE POUR LES BALKANS OCCIDENTAUX (VERSION D'OCTOBRE 2023)**

*La Stratégie interministérielle pour les Balkans occidentaux est née de la volonté du président de la République de réengager la France pour la stabilisation des six pays des Balkans occidentaux, pour leur développement économique et social et pour le renforcement de l'État de droit, dans la perspective de leur adhésion à l'Union européenne.*

Elle repose sur le constat que depuis le début des années 2000 et la fin des conflits armés liés à l'éclatement de la Yougoslavie, les pays de la région n'ont pas progressé de manière décisive vers l'Union européenne en raison de nombreux défis politiques, économiques, démocratiques et sécuritaires.

Depuis son lancement en 2019, la Stratégie française pour les Balkans occidentaux a connu une évolution sensible liée notamment :

- à la guerre d'agression russe en Ukraine et à l'accentuation consécutive des difficultés économiques et sociales de la région, dans un climat de polarisation et de déstabilisation encouragé par des entreprises de désinformation et la multiplication du nombre de cyberattaques d'ampleur ;
- à l'évolution de la politique d'élargissement de l'Union européenne, devenue plus politique, plus dynamique et plus incitative, à la faveur de la nouvelle méthodologie des négociations d'adhésion promue par la France ;
- à la persistance, voire l'aggravation des crises régionales requérant l'engagement de la France au plus haut niveau afin d'apporter des propositions de résolution des différends.

La France entend renforcer sa coopération bilatérale avec tous les pays de la région et sa contribution à la coopération régionale, avec plusieurs priorités dont i) la mise en œuvre de l'Agenda vert et la transition énergétique et numérique ii) la lutte contre la désinformation et les menaces cyber, iii) le soutien à la société civile, iv) l'appui aux administrations, présumé indispensable à la réussite des réformes dans le cadre du processus d'adhésion.

Le président de la République s'est exprimé à Bratislava et plus récemment à Tirana pour rappeler que la France soutient résolument la perspective européenne des pays des Balkans occidentaux et souhaite que l'Union européenne poursuive et renforce son soutien pour aider la région à avancer rapidement sur la voie des réformes nécessaires à son rapprochement européen, conformément à la nouvelle méthodologie de l'élargissement. L'intégration des pays des Balkans occidentaux, qui participe à la réunification du continent européen, est souhaitée par la France le plus rapidement possible.

## **Mesures concrètes.**

### **I. La France a intensifié le dialogue politique avec les pays de la région.**

Le président de la République s'est rendu en Serbie en juillet 2019 et en Albanie en octobre 2023. La secrétaire d'État chargée de l'Europe, Laurence Boone, s'est rendue plusieurs fois en Albanie (novembre 2022 et octobre 2023), en Macédoine du Nord (novembre 2022 et juillet 2023) ainsi qu'en Bosnie-Herzégovine (mars 2023). Le ministre délégué chargé du commerce et de l'attractivité, Olivier Becht, a effectué un déplacement en Macédoine du Nord, Serbie et Albanie en septembre 2023 et s'est rendu à nouveau en Albanie en octobre 2023.

D'autres visites, notamment de parlementaires, dans tous les pays de la région, ont également contribué à l'intensification de nos relations politiques.

Les autorités des pays de la région sont régulièrement reçues à Paris, notamment à l'occasion du Forum de Paris pour la Paix.

La France s'implique, à haut niveau, dans la résolution des crises régionales, en particulier dans le dialogue entre la Serbie et le Kosovo, en appui à la médiation européenne (rencontres en marge des sommets de la Communauté politique européenne – CPE – à Prague, Chisinau et de Grenade), mais également en débloquent sous la Présidence française de l'Union européenne le différend entre la Bulgarie et la Macédoine du Nord, permettant à cette dernière d'ouvrir la première phase des négociations d'adhésion avec l'Union européenne.

La France a nommé en octobre 2023 un envoyé spécial pour les Balkans occidentaux.

### **II. La France a renforcé sa coopération bilatérale avec les pays de la région dans cinq domaines :**

#### **1. Présence et influence économique, notamment avec l'intervention de l'Agence française de développement**

- Signature de cinq accords intergouvernementaux depuis 2019 pour permettre l'intervention de l'AFD en Albanie, au Kosovo, au Monténégro, en Macédoine du Nord et en Serbie.
- Engagement par l'AFD de plus de 1,1 milliard d'euros depuis 2019 dans les Balkans occidentaux au service de la transition écologique et en soutien de l'intégration régionale et du rapprochement européen des pays des Balkans occidentaux.
- Mise à disposition de 12 Experts techniques internationaux (ETI) au sein des administrations des pays de la région sur des fonctions stratégiques, notamment l'intégration européenne et l'appui à l'agenda vert.

- Soutien apporté par la DGAFP à la coopération dans le domaine administratif pour renforcer les capacités des pays de la région dans ce domaine.
- Mobilisation des outils de financement export (Fonds d'études et d'aide au secteur privé – FASEP et prêts du Trésor) pour la réalisation de projets stratégiques dans les domaines de la biodiversité, de la gestion des déchets, de l'énergie et de la santé.
- Renforcement de la présence du ministère de l'agriculture et de la souveraineté alimentaire avec la création d'un poste de conseiller pour les affaires agricoles à Belgrade.
- Création à Belgrade d'un poste de conseiller régional rattaché au ministère de la transition écologique.
- Augmentation des échanges commerciaux avec les Balkans occidentaux (+77 % en cinq ans).
- Réimplantation prochaine d'un bureau Business France en Grèce, ayant compétence sur les Balkans occidentaux.

## 2. Sécurité

- Lutte contre les trafics illicites d'armes légères et de petit calibre (ALPC) : la mise en œuvre de la feuille de route franco-allemande visant à mobiliser les pays de la région et à coordonner l'assistance de la communauté internationale pour lutter contre le trafic d'armes s'est poursuivie. Les six États des Balkans occidentaux ont bénéficié de la donation par la France de systèmes de comparaison balistique (EVOFINDER) et de logiciels de renseignement criminalistique (TRAFFIC), mais aussi de formations.
- **Cybersécurité et lutte contre la cybercriminalité : lancement des premières formations du centre de développement des capacités cyber dans les Balkans occidentaux (C3BO) en mai 2023 et signature en octobre 2023 d'un traité visant à lui octroyer le statut d'organisation internationale.**
- Coopération bilatérale en matière de sécurité intérieure : des unités permanentes de renseignement criminel (UPRC) ont été mises en place et le dispositif sur le terrain du ministère de l'intérieur s'est renforcé.
- Lutte contre le terrorisme et la radicalisation : soutien à la mise en place de plateformes de signalement de contenus illicites sur internet (PHAROS).
- Lutte contre la traite des êtres humains : des actions de coopération technique et opérationnelle sont mises en œuvre, visant à favoriser le renforcement des capacités, la prévention, la protection des victimes et le démantèlement des réseaux criminels, dans le cadre de la stratégie interministérielle de

coopération en matière de lutte contre la traite des êtres humains en Europe du Sud-Est.

### **3. Défense**

- Intensification de la coopération de défense avec les pays de la région, avec plusieurs dialogues stratégiques au niveau national (Serbie, Macédoine du Nord, Bosnie-Herzégovine) et des visites d'autorités militaires.
- Réengagement dans l'opération EUFOR-Althéa depuis mars 2019 avec un détachement d'une vingtaine de soldats français. La force EUFOR-Althéa est sous commandement stratégique français (Vice-Shape, Général Cottureau).
- Signature d'un accord intergouvernemental de défense avec la Macédoine du Nord en octobre 2022.
- Formations d'officiers des pays des Balkans occidentaux dans les écoles françaises de formation et de ressortissants de ces États à l'Institut des hautes études de la défense nationale (IHEDN).
- Coopération opérationnelle en soutien à l'engagement des pays des Balkans occidentaux dans des opérations extérieures à nos côtés.

### **4. Justice**

- Accompagnement des réformes engagées au titre du processus d'adhésion à l'Union européenne avec la mise en œuvre de la deuxième phase du projet EU4Justice (2022-2025) en Bosnie-Herzégovine et la participation à la phase VI du projet européen EURALIUS en Albanie.
- Poursuite de la coopération technique en matière de lutte contre le trafic de stupéfiants, d'armes et la traite des êtres humains, et de lutte contre la criminalité organisée et la corruption, par l'organisation de conférences et la formation de magistrats des pays de la région.
- Mise en place de nouvelles coopérations en matière de criminalité financière et économique, de lutte contre les trafics de biens culturels et d'espèces protégées, de criminalité environnementale qui peuvent également constituer des sources de financement du terrorisme.
- Constitution d'équipes communes d'enquête avec tous les pays de la région.

### **5. Culture, éducation, langue française et jeunesse**

- Renforcement de la coopération culturelle avec des financements de projets régionaux sur l'éducation aux médias et la lutte contre la désinformation. Le relais spécialisé régional pour le spectacle vivant Teatroskop s'est poursuivi. La France a participé à Novi Sad 2022 capitale européenne de la culture. Des

accords de coopération cinématographique ont été signés. Lancement en octobre 2023 du nouvel Institut français d’Albanie « KubFrance-Tirana ».

- Renforcement de la coopération universitaire par le développement des bourses du gouvernement français et la signature d’accords de coopération entre des universités françaises et des Balkans occidentaux.
- Promotion de la langue française avec des financements (Fonds de solidarité pour les projets innovants – FSPI) visant à consolider l’enseignement du français à tous les niveaux (enseignement primaire, secondaire, universitaire et au niveau des administrations) dans l’ensemble des pays de la région.
- Création d’un poste d’attaché audiovisuel régional à Belgrade.
- France, invitée d’honneur du salon du livre de Belgrade et lancement d’un FSPI-R dans le domaine de l’édition.
- Financement de 11 projets dans le cadre du Fonds Équipe France (ex-FSPI) afin d’accompagner les initiatives de coopération académique des établissements et centres de recherche français dans les Balkans occidentaux.
- Participation et contribution financière en 2023 au lancement du campus de Tirana du Collège de l’Europe (octobre 2023).
- Poursuite du soutien à des projets dans le domaine de l’égalité femmes/hommes, de la réconciliation et de la jeunesse, et en appui à la société civile, au travers de l’Office régional de coopération pour la jeunesse (RYCO), à travers un incubateur régional d’entreprises sociales, la promotion et la protection des droits des LGBTI+ et la protection de l’environnement. La France a soutenu en 2022-2023 ces projets à hauteur de 1,9 million d’euros.