N° 284

SÉNAT

SESSION ORDINAIRE DE 2024-2025

Enregistré à la Présidence du Sénat le 29 janvier 2025

RAPPORT

FAIT

*au nom de la commission des affaires étrangères, de la défense et des forces armées (1) sur le projet de loi autorisant l'***approbation** *de l'***accord** *portant* **création** *du* **Centre** *de* **développement** *des* **capacités cyber** *dans les* **Balkans occidentaux** *(C3BO),*

Par Mme Sylvie GOY-CHAVENT,

Sénateur

(1) Cette commission est composée de : M. Cédric Perrin*, président ;* MM. Pascal Allizard, Olivier Cadic, Mmes Hélène Conway-Mouret, Catherine Dumas, Michelle Gréaume, MM. André Guiol, Jean-Baptiste Lemoyne, Claude Malhuret, Akli Mellouli, Philippe Paul, Rachid Temal*, vice-présidents ;* M. François Bonneau, Mme Vivette Lopez, MM. Hugues Saury, Jean-Marc Vayssouze-Faure*, secrétaires ;* MM. Étienne Blanc, Gilbert Bouchet, Mme Valérie Boyer, M. Christian Cambon, Mme Marie-Arlette Carlotti, MM. Alain Cazabonne, Olivier Cigolotti, Édouard Courtial, Jérôme Darras, Mme Nicole Duranton, MM. Philippe Folliot, Guillaume Gontard, Mme Sylvie Goy-Chavent, MM. Jean-Pierre Grand, Joël Guerriau, Ludovic Haye, Loïc Hervé, Alain Houpert, Patrice Joly, Mmes Gisèle Jourda, Mireille Jouve, MM. Alain Joyandet, Roger Karoutchi, Ronan Le Gleut, Didier Marie, Thierry Meignen, Jean-Jacques Panunzi, Mme Évelyne Perrot, MM. Stéphane Ravier, Jean-Luc Ruelle, Bruno Sido, Mickaël Vallet, Robert Wienie Xowie.

Voir les numéros :

Sénat : **166** et **285** (2024-2025)

SOMMAIRE

Pages

L'ESSENTIEL

Le présent projet de loi a pour objet l'approbation de l'accord, signé à Tirana le 16 octobre 2023 entre le gouvernement de la République française, le Monténégro et la République de Slovénie, relatif à la création d'un Centre de développement des capacités cyber dans les Balkans occidentaux (soit : l'Albanie, la Bosnie-Herzégovine, le Kosovo, la Macédoine du Nord, le Monténégro, et la Serbie), dit « C3BO » ; cet accord permet notamment de conférer au C3BO le statut d'organisation internationale.

La cybersécurité constitue dorénavant un enjeu majeur de l'environnement numérique mondial, avec une montée en puissance fulgurante, tant qualitative que quantitative, des capacités d'agression. Face à de telles attaques, à défaut d'une politique de cyber-résilience robuste, des États entiers peuvent se trouver ébranlés, comme le Monténégro et l'Albanie en firent l'expérience en 2022, à leurs dépens.

Les pays des Balkans occidentaux font en effet figure de cibles faciles, du fait de l'insuffisance de leur culture en matière de cybersécurité et de leur difficulté à former et retenir les compétences en la matière. Or de ce fait, ils créent un risque de compromission par rebond de notre propre cyberespace, national, européen, et atlantiste.

Si l'ensemble de la région aspire à un rapprochement, voire à une intégration, avec l'Union européenne et l'OTAN, ce tropisme euro-atlantiste s'érode peu à peu, du fait de l'attente délétère de ces pays dans l'antichambre européenne, mais aussi du jeu d'influences et d'ingérences très agressif dont ils font l'objet de la part notamment de la Russie.

C'est pourquoi le C3BO faisant l'objet du présent projet de loi apparaît comme une initiative particulièrement opportune de la France et de la Slovénie : le Centre, implanté à Podgorica (Monténégro), dispensera cette année 31 formations par an dans les domaines de la cybersécurité, au bénéfice de quelque 600 stagiaires originaires de la région, pour un coût global de 1,05 millions €, dont 870 000 € (83%) à la charge de la France. A cet égard, le C3BO est porteur d'un signal d'autant plus fort qu'il permet également, en même temps qu'il améliore le niveau de résilience cyber des Balkans occidentaux et alimente le partenariat entre la France et cette région d'importance géostratégique majeure, de la rapprocher des standards de l'Union européenne et notamment de la directive NIS2.

Enfin ce Centre participe au « *soft power* » français : avec des compétences qui lui permettent de se positionner à l'échelle internationale comme une puissance cyber de premier rang, responsable, coopérative et solidaire, la France tire de son rôle cyber-diplomatique un bénéfice réputationnel important, auquel le C3BO viendra assurément contribuer.

L'objet de cet accord est d'autoriser la transformation de l'actuel C3BO en organisation internationale. Ce statut devrait permettre de renforcer la sécurité juridique du centre en lui conférant une personnalité juridique internationale, dotée d'un conseil d'administration, d'une gouvernance et d'un financement dédiés. La France, la Slovénie et le Monténégro en seraient les membres fondateurs ; les 5 autres pays des Balkans occidentaux ont vocation à en devenir membres ; l'accord prévoit en outre qu'ils pourraient être rejoints le cas échéant par d'autres pays européens. La future organisation internationale présentera notamment l'avantage, par rapport au format actuel, de permettre un financement par ces futurs autres membres et, à terme, par l'Union européenne.

La commission des affaires étrangères, de la défense et des forces armées a adopté ce projet de loi, dont le Sénat est saisi en premier, assorti de deux recommandations d'ordre financier.

I. APPROCHE CONTEXTUELLE

A. LA CYBERSÉCURITÉ : UN ENJEU CRITIQUE

Le développement croissant des usages du numérique depuis une vingtaine d'années a forgé, *de facto* et en l'absence de toute architecture structurante préétablie – un nouveau concept en même temps qu'une nouvelle réalité, appelée « cyberespace »[1] . Défini par l'interconnexion mondiale de l'ensemble des équipements, applications et données numériques, on considère habituellement qu'il est composé de trois couches :

- Matérielle, englobant tant les infrastructures telles les câbles sous-marins, les satellites, les *datas centers*, que les ordinateurs, smartphones et l'ensemble des appareils connectés.
- Logicielle, permettant le fonctionnement du matériel physique connecté.
- Informationnelle, c'est-à-dire les données en circulation.

A l'heure où la bonne marche d'un État (dans les domaines logistique, médical, commercial, administratif, financier… mais aussi policier et militaire) s'identifie à celle de son cyberespace, la dépendance de nos sociétés au bon fonctionnement de leurs services numériques constitue une donnée irréversible de la modernité.

L'apparition de cet environnement numérique planétaire, caractérisé tant par son absence de frontière que par son absence de régulation, s'est vu accompagné par celle de nouvelles menaces, concernant potentiellement chacune de ses trois couches. L'extension du cyberespace, et donc des surfaces d'attaque potentielle offerte aux agresseurs, ainsi que l'interdépendance des États au sein de cet espace, constituent à cet égard autant d'opportunités pour nos adversaires, qu'ils soient étatiques ou non-étatiques : visées criminelles, espionnage, déstabilisation, ingérence ou guerre hybride...

Les panoramas de la menace 2022 et 2023 de l'ANSSI mettent en lumière une évolution de la menace cyber, qui, alors qu'elle se concentrait précédemment sur les acteurs et opérateurs stratégiques, **ciblent désormais le tissu social et économique de manière indifférenciée : ainsi, en 2023 en France, 69 % des cyberattaques visaient des entreprises, 20 % concernaient des collectivités territoriales et 11 % des établissements de santé.**

Les différents scenarios-catastrophe que l'on a connus récemment au Monténégro, en Albanie, mais aussi en Union européenne ou Etats-Unis, ont fait la preuve, s'il était besoin, de l'extrême capacité de nuisance de telles attaques.

---

[1] *Le terme tire son origine du roman de science-fiction dystopique Neuromancien (1984), de William Gibson.*

Le domaine cyber constitue désormais l'un des enjeux géostratégiques majeurs et fait partie intégrante des rapports de force qui régissent les relations internationales.

1. Les différentes facettes de la menace cyber

La notion d'« attaque cyber », qui se caractérise par l'infiltration d'un système informatique dans un but malveillant, recouvre une typologie variée d'actes, différant par leurs modes opératoires, leurs auteurs, leurs objectifs… et qu'il convient de distinguer.

a) Les « cyber-agresseurs », ou les nouveaux visages du danger

La menace cyber se caractérise par l'hétérogénéité de ses attaquants ; on distingue généralement parmi eux trois grandes catégories d'agresseurs, allant de l'échelle de l'individu à l'échelle étatique.

Pour autant, cette hétérogénéité n'exclut pas une certaine porosité entre les trois catégories : ainsi la compétence technique des « hacktivistes » opérant en « zone grise » est particulièrement prisée, tant par les services étatiques que par les criminels, qui sont également intéressés pour les recruter.

- ***États et agences de renseignement : les acteurs masqués d'une guerre non assumée***

Les États et leurs agences de renseignement, du fait des importantes ressources humaines et matérielles dont elles disposent, ont la capacité de réaliser des opérations offensives de grande ampleur et de longue durée. L'évolution géopolitique des dernières années a vu la montée en puissance de différents États qui se sont engagés dans une guerre hybride prenant pour cible, notamment, les démocraties occidentales dont la France.

De telles agressions recouvrent un large panel d'actions, pouvant aller des **attaques réputationnelles, dont l'ampleur et l'impact sont variables et difficilement quantifiables, à des offensives majeures et spectaculaires**, telle la cyberattaque dont a été victime le Monténégro en août 2022, ou les ingérences électorales directes récemment avérées.

Certaines opérations d'influence reposent sur la compromission de contenus légitimes (boîtes mails, sites internet) afin de pouvoir diffuser des contenus altérés (« *fake news* »). D'autres attaques chercheront à empêcher le fonctionnement des sites officiels (« déni de service »). Pour les auteurs de ces opérations, il s'agit avant tout de modifier les perceptions d'une population et de déstabiliser un acteur donné ou un processus démocratique.

Pour ne citer que l'offensive la plus récente, dans notre pays, le 31 décembre dernier, les infrastructures numériques de plusieurs villes et départements français ont fait l'objet d'une attaque coordonnée : Marseille, Bordeaux, Nantes, Nice, Pau, Poitiers ou encore Tarbes ont vu leurs sites

rendus inaccessibles. Le lendemain, d'autres entités comme la ville de Montpellier, les départements de l'Aude et de l'Eure, ainsi que la région Centre-Val-de-Loire rejoignaient la liste des collectivités touchées. Selon les informations disponibles, ces actes malveillants seraient attribués au groupe de hackers pro-russe *NoName05716*.

De telles attaques, qui recherchent généralement une visibilité maximale, **relèvent souvent de la démonstration de force** ; **elles visent, en renvoyant une image délétère de la sécurité d'un État, à fragiliser ses institutions ou ses dirigeants**. Au-delà de leurs conséquences immédiates, leur récurrence constitue également en soi un préjudice, par son impact psychologique déstabilisateur. Plusieurs États s'illustrent notoirement dans de telles activités hostiles – Russie, Chine, Azerbaïdjan, Iran, Turquie… notamment.

Inversement, **les attaques à fins d'espionnage ont vocation à demeurer invisibles** de façon à prolonger le plus longtemps possible l'accès aux informations ciblées. Elles peuvent viser tant des institutions, services de l'État, ou installations critiques, que des entreprises privées (espionnage industriel). Elles ont pour objectif, dans le premier cas, de pirater des renseignements stratégiques ou militaires, ou encore, dans le second, d'accéder à des données techniques, financières ou commerciales, à des informations concernant des brevets ou des marchés publics... On soulignera que les auteurs de telles attaques, loin de se limiter à nos compétiteurs identifiés comme tels, sont **bien souvent des pays considérés comme alliés de la France**.

- ***Les « Hacktivistes » : des « chapeaux blancs » aux « chapeaux noirs », cinquante nuances de gris***

Le mot-valise « hacktiviste » - contraction de « *hacker* » et « activiste » - désigne un individu, ou collectif d'individus, qui va chercher à infiltrer illégalement des réseaux informatiques à des fins militantes, de façon à diffuser une critique ciblée à l'encontre de personnalités, d'entreprises, de politiques, d'opinions[1]…

En fonction des motivations plus ou moins éthiques des *hackers*, on parlera de « *white hat hacker* » ou de « *grey hat hacker* ». La première catégorie recouvre une catégorie de métiers oeuvrant légalement à la recherche des failles fragilisant les logiciels et les systèmes informatiques ; ils s'opposent aux cybercriminels, ou « *black hat hackers* ».

---

[1] *Les plus connus sont : Anonymous,(célèbres pour leurs actions visant l'Eglise de scientologie, et de nombreux régimes dictatoriaux ; ils ont notamment piraté le site du Kremlin en 2022), Cult of the dead cow, LulzSec… ; on compte aussi des groupes d'inspiration nationaliste ou religieuse : IDF team, actif pour défendre l'Etat d'Israël, The Jester, en faveur des États-Unis d'Amérique, l'Armée électronique syrienne de Bachar el Assad, les groupes d'hacktivisme djihadistes Izz ad-Din al Qassam Cyber Fighter ou OxOmar…*

Les hacktivistes sont généralement considérés comme des "*grey hats hackers*", oscillant entre le monde des « blancs » et celui des « noirs » : plus sensibles à la légitimité d'une action qu'à sa stricte légalité, ils sont susceptibles de basculer d'un côté ou de l'autre en fonction des intérêts qu'ils défendent ou des comportements qu'ils dénoncent.

Les hacktivistes recourent aux mêmes procédés que les *hackers* dits « noirs » : piratages, détournements de serveurs, « défacements » (remplacement d'une page d'accueil par un message), censure de messages, « *géo-bombings* » (ajout d'un tag à une vidéo permettant aux spectateurs de géolocaliser le lieu où elle a été prise), déni de services… *etc*, mais au nom d'une éthique qui leur est propre, volontiers libertaire, anti-système, anti-capitaliste... Certains hacktivistes deviennent également des lanceurs d'alertes[1] en diffusant des données confidentielles obtenues par piratage, afin de dénoncer à l'opinion publique certains agissements.

- ***Les organisations criminelles, ou la montée en puissance d'un écosystème de mieux en mieux structuré***

Du fait de sa très grande vulnérabilité et, en même temps, de son caractère vital pour les États modernes, l'espace cyber est particulièrement exposé aux attaques à vocation criminelle qui vont chercher, dans un but lucratif, à en exploiter les faiblesses.

Leur finalité étant exclusivement l'appât du gain, leur ciblage est large et essentiellement opportuniste : entreprises, administrations et services de l'État, associations, établissements de santé, secteur de l'énergie et des télécommunications… mais aussi particuliers, constituent pour eux un immense vivier de victimes potentielles. Les PME sont particulièrement vulnérables, en raison des ressources limitées qu'elles peuvent généralement consacrer à la cybersécurité : c'est ainsi que le nombre d'entreprises de moins de dix salariés ayant subi une cyberattaque a augmenté de plus de 50% entre 2020 et 2023[2]. Les grandes entreprises, les infrastructures stratégiques, les opérateurs téléphoniques, les institutions ou services publiques constituent des cibles de choix du fait du montant important de la potentielle rançon exigible[3]. Enfin les particuliers font l'objet de sollicitations malveillantes multiples (*phishing* par courriel ou sms, appel d'un faux conseiller bancaire…) et de plus en plus élaborées.

---

[1] *On rappellera les Wikileaks, de Julian Assange (2006) ou les révélations d'Edward Snowden (2013).*
[2] *Source : www.data.gouv.fr.*
[3] *A titre d'exemple, en avril 2021, la société américaine Colonial Pipeline, qui alimente en carburant 45% de la Côte Est des Etats-Unis, a subi une importante attaque par rançongiciel qui a entraîné une rupture d'approvisionnement générant une panique chez les habitants de la région, puis une pénurie. Colonial Pipeline a alors payé une rançon de 4,4 millions de dollars en bitcoin en échange de la clef de déchiffrement des fichiers dérobés et cryptés par les cyber-pirates.*

Le cybercriminel poursuit un profit financier à un triple niveau :

- Suite à l'introduction d'un logiciel malveillant de chiffrement rendant inopérationnel le système informatique de la victime, une rançon est exigée en échange de la clé de chiffrement.
- Après vol des données de la victime, une rançon est exigée sous menace de les diffuser.
- La vente des données piratées.

Les conséquences de telles attaques sont très lourdes, notamment pour les PME, qui sortent bien souvent durablement fragilisées par l'incident, allant parfois jusqu'au dépôt de bilan[1].

b) Une évolution inquiétante…

Plusieurs évolutions récentes contribuent à aggraver l'acuité de la menace :

Tout d'abord la sophistication croissante des attaques, à la faveur notamment des multiples possibilités ouvertes par l'intelligence artificielle : ainsi, aux approximations concernant la grammaire, le contenu ou la charte graphique des messages, aux sollicitations téléphoniques maladroites, qui antérieurement ne manquaient pas de trahir des tentatives d'extorsion le plus souvent grossières, se sont peu à peu substitué des communications impeccables, reprenant dorénavant à la perfection tous les codes des messages écrits, ou reproduisant à s'y méprendre des voix ou même des visages en visioconférence.

Les « fermes » ou « usines à trolls » ont été développées par certains États[2] dans le but de répandre sur internet de fausses nouvelles et de mener des opérations de propagande. On citera notamment la *Research Agency* russe, qui est notamment soupçonnée d'avoir pesé sur les élections américaines de 2016 et sur le vote du Brexit. En Chine, ce sont des dizaines de milliers de faux comptes qui ont été identifiés, puis fermés par Facebook, Twitter et YouTube. D'autres États comme l'Iran utilisent des « trolls » à des fins de propagande intérieure. Avec **l'émergence des « *bots* » (robots numériques), le développement de l'intelligence artificielle et l'appui des algorithmes des réseaux sociaux** dont les « trolls » maîtrisent les subtilités, leur influence s'est décuplée.

Par ailleurs, alors que la conduite d'une cyberattaque requérait antérieurement un certain de degré de compétence en matière informatique, **il existe à présent des « *kits* d'attaque » facilement accessibles en ligne sur**

---

[1] *Aucune statistique fiable ne permet d'évaluer le taux d'entreprises ou d'établissements attaqués se pliant à l'exigence de rançon. L'ANSSI déconseille vivement aux victimes de céder au chantage en raison de l'absence de garantie offerte par l'agresseur.*

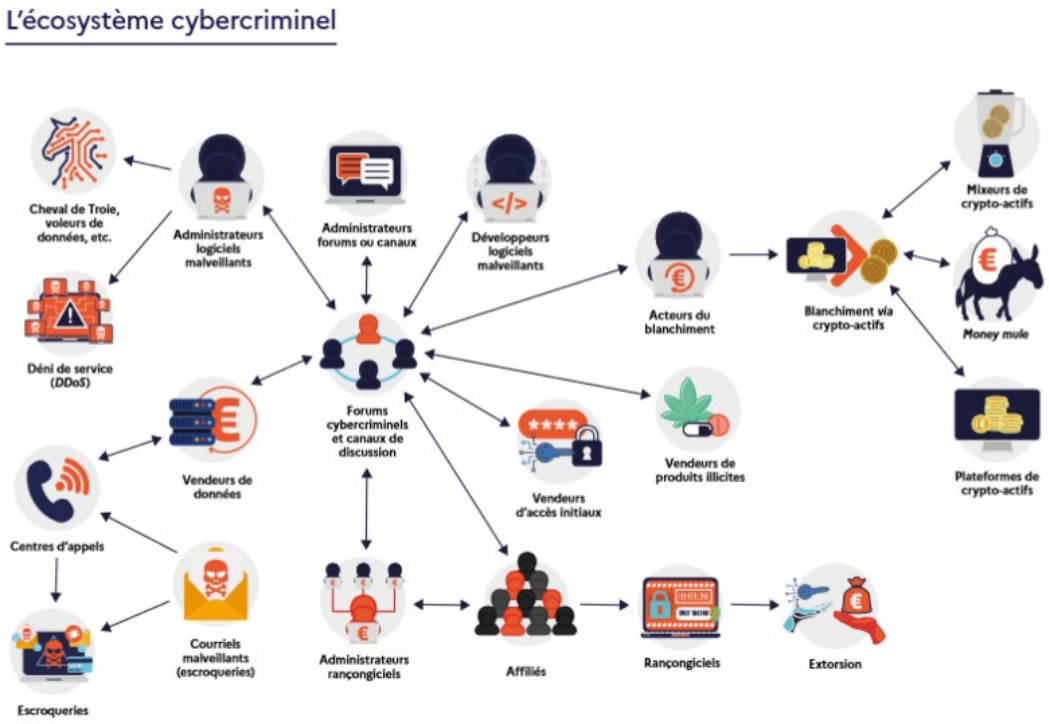
[2] *D'après l'ONG américaine* Freedom House*, au moins 30 États auraient lancé des campagnes de désinformation dans le but de discréditer le modèle démocratique en 2017 ; 18 scrutins électoraux auraient été visés.*

le *darknet*, mettant à la portée d'internautes de tous niveaux des rançongiciels prêts à l'emploi. Ce phénomène, qui s'est considéré amplifié récemment, a pour effet de grossir la population d'agresseurs potentiels.

Le cyberespace a vu également apparaître de **véritables officines, d'un très bon niveau technique, proposant de véritables services de piratage** à leurs clients : outils clé en main, mais aussi offres d'expertise personnalisées ou analyses de vulnérabilités « *0-Day* ». Si ces services sont généralement réservés à des clients étatiques dans le cadre de la lutte contre le terrorisme et la criminalité organisée, ils peuvent être détournés à des fins d'espionnage.

Enfin le milieu des cybercriminels est de plus en plus structuré, avec **des forums permettant l'échange de données, la vente de logiciels malveillants en ligne, mais aussi des liens vers des entreprises spécialisées dans la vente de prestations et de services cyber-offensifs ou des circuits de blanchiment**…

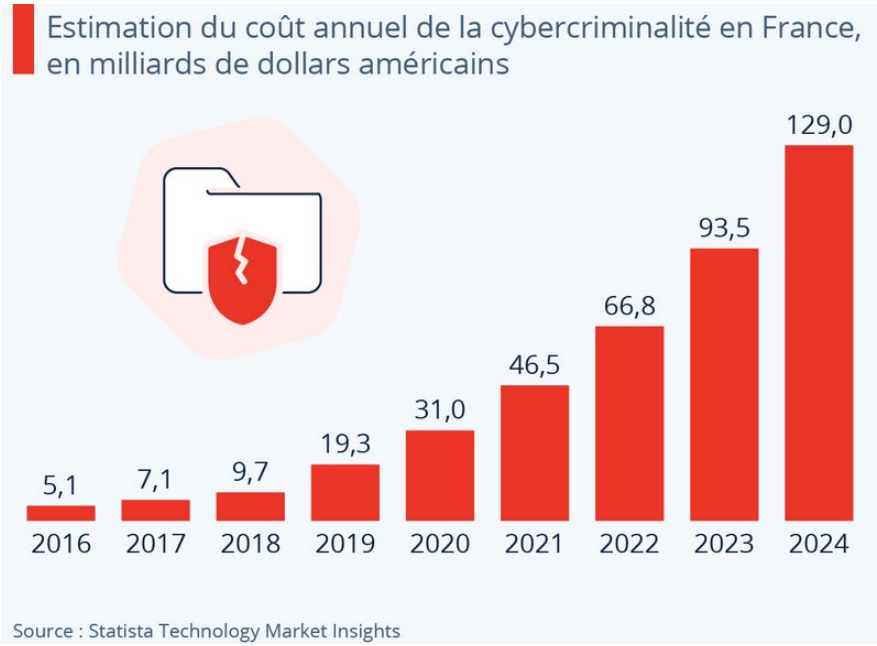
Le Rapport sur la cybercriminalité 2024 du Ministère de l'Intérieur et des Outre-mer modélise comme suit ce qu'il décrit comme un « **écosystème cybercriminel** » :



Exemple de modélisation d'un écosystème cybercriminel

Compte tenu du fait que leur impunité est notoirement importante et leur succès potentiellement très lucratif à peu de frais, **les cyberattaques font figure de délit particulièrement rentable**.

Ces éléments expliquent l'inexorable inflation du nombre des attaques et de leur coût, et ne laissent entrevoir, à court et moyen terme, aucune perspective de décrue, bien au contraire :



A l'échelle mondiale, le coût de la cybercriminalité est estimé en 2024, par le même institut, à 9,22 milliers de milliards de dollars ; à horizon 2029, il pourrait atteindre 15,63 milliers de milliards de dollars.

c) … avec une panoplie de modes opératoires…

Différents logiciels malveillants (« *malwares* ») ont été élaborés par les cybercriminels pour parvenir à leurs fins :

- **Virus** : logiciel permettant d'infecter un réseau, par corruption ou destruction de données ou en endommageant le système.
- **Ver informatique** : variante du virus, se propageant de manière autonome, souvent *via* des réseaux.
- **Rançongiciel** : logiciel chiffrant les données dans le but d'obtenir une rançon pour les décrypter.
- **Logiciel espion** : logiciel permettant de collecter des informations sans le consentement de l'utilisateur.
- **Cheval de Troie** : logiciel en apparence légitime, mais qui contient, à l'insu de son utilisateur, une fonctionnalité malveillante.
- ***Rootkits*** : logiciel permettant à un attaquant de prendre le contrôle total d'un système sans être détecté.

Les principaux modes opératoires employés par les agresseurs pour accéder aux données, ou infecter le système informatique de leur victime par des logiciels malveillants peuvent se classer comme suit :

➢ *Attaques par hameçonnage et ingénierie sociale*

- **Hameçonnage (« *phishing* »)** : technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans un but d'usurpation d'identité. L'agresseur fait ainsi croire à la victime, par un courriel ou un SMS frauduleux, qu'elle est en contact avec un tiers de confiance — banque, administration, entreprise… — afin de lui soutirer mot de passe, numéro de carte de crédit, numéro ou photocopie de la carte d'identité, date de naissance… Le plus souvent, une copie exacte d'un site web est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site web officiel où elle pensait se connecter.
- **« *Pretexting* »** : forme d'ingénierie sociale par laquelle un cyberattaquant utilise un leurre, ou un scenario fictif (par exemple en se faisant passer pour un investisseur, un responsable RH, un spécialiste informatique ou toute autre autorité légitime) pour gagner la confiance de la victime et obtenir l'accès à des données confidentielles, à un système ou à un service.
- **« *Baiting* »** : utilisation d'appâts -plus souvent des clés USB infectées - qui vont à leur tour contaminer les ordinateurs auxquels elles seront connectées.

➢ *Attaques par déni de service (DoS) et déni de service distribué (DDoS)*

- **Déni de service (« *denial of service* » : DoS)** : Surcharge un système ou un réseau rendant ainsi un site Web ou une ressource indisponible.
- **Déni de service distribué (« *Distributed denial of service* » : DDoS)** : variante de DoS utilisant plusieurs machines distantes (« zombies » ou robots) pour mener l'attaque.

➢ *Intrusion dans les réseaux*

- **Attaque de l'« homme du milieu » (« *Man-in-the-Middle* » : MitM)** : Interception et manipulation des communications entre deux parties, souvent par le biais d'un réseau *wi-fi* ouvert. L'attaquant s'installe alors au sein du système d'exploitation dans le but d'intercepter des données telles que les identifiants de connexion.
- **Écoute de communications ou « reniflement » de données** : Espionnage passif ou actif *via* des commutateurs « *switch* ».

➢ *Exploitation de vulnérabilités logicielles*

- **Exploits** : Utilisation de failles connues pour compromettre un système.
- **Vulnérabilité « du jour zéro » (« *0-Day* »)** : Exploitation de failles inconnues des développeurs.

- ***Attaques ciblant les mots de passe***

- **« Force brute »** : Essai systématique de toutes les combinaisons possibles.
- **Attaque par dictionnaire** : Test de mots de passe courants ou prévisibles.
- **« *Credential stuffing* »** : Utilisation d'identifiants volés sur d'autres services.

- ***Attaques* via *chaînes d'approvisionnement***

- **Compromission des fournisseurs ou des partenaires** d'une organisation pour atteindre la cible principale. Cette méthode présente un risque de propagation rapide d'une attaque qui peut parfois concerner un secteur d'activité entier ou une zone géographique précise notamment lorsque l'attaque cible un fournisseur de logiciels largement répandus, une entreprise de service numérique (ESN) locale ou spécialisée dans un secteur d'activité particulier.

- ***Attaque par point d'eau***

- **L'attaque par point d'eau (« *watering hole* »)** consiste à piéger un site internet légitime afin d'infecter les équipements informatiques des visiteurs.

- ***Défiguration de sites internet***

- Ce type d'attaque tend à ajouter ou modifier des informations dans une page web à des fins de revendications. Ces opérations, qui exploitent souvent des vulnérabilités connues mais non corrigées, sont généralement revendiquées par des hacktivistes pour motifs politiques ou idéologiques, ou à des fins de défi technique entre attaquants.

d) <u>L'épée de Damoclès de l'informatique quantique</u>

À ce tableau déjà très préoccupant s'ajoute la **perspective du développement de technologies quantiques**[1] – à horizon 2030 ou 2040[2]. Cette évolution, qui devrait révolutionner l'informatique, représente une menace majeure en termes de cybersécurité : L'ANSSI alerte ainsi contre un prévisible « *effondrement de la sécurité de la cryptographie à clé publique actuellement*

[1] *La principale différence entre les ordinateurs classiques et quantum est que ces derniers utilisent au lieu de bits* ***des qubits qui peuvent être utilisés en superposition****, ce qui permet de multiplier exponentiellement leur capacité. À titre d'exemple, le processeur quantique expérimental Willow a pu résoudre en moins de cinq minutes un calcul qui prendrait dix septillions d'années à Frontier, l'un des supercalculateurs actuels les plus puissants au monde.*

[2] *À l'heure actuelle, le processeur quantique est encore au stade exploratoire : son encombrement est de l'ordre de 3 m x 2 m x 2 m. Un vide très poussé, de 10-11 mbar, est également nécessaire – ce qui correspond à peu près à la pression à la surface de la lune.*

déployée »[1]. En effet, les algorithmes de cryptographie utilisés pour sécuriser les communications, les transactions financières et les données sensibles s'avéreraient inefficaces face à un processeur quantique. **Le défi de la cybersécurité sera ainsi de déployer au plus vite – avant l'aboutissement de la transition vers de tels processeurs - une cryptographie post-quantique robuste**.

2. Face à ces agressions, quelles parades ?

On parle volontiers de « **cyber-résilience** »[2], concept impliquant d'accepter que les violations soient inévitables et de choisir de se préparer à l'événement à l'avance.

L'erreur humaine est en effet responsable de 90 % des cyberattaques[3] : Clics sur des liens malveillants, utilisation de mots de passe faibles ou partagés, partage imprudent d'informations sensibles, négligence dans la mise à jour des logiciels et systèmes, erreurs de configuration et mauvaise gestion des accès, utilisation négligente de clés USB… constituent autant d'imprudences qui mettent en péril la sécurité d'un système d'information.

C'est pourquoi la prévention et l'éducation à la cybersécurité jouent un rôle déterminant dans la cyber-résilience d'un État, afin de sensibiliser un public le plus large possible aux bonnes pratiques numériques.

Or cette culture de la cybersécurité est très inégalement intégrée selon les pays. Si la France, forte d'une expertise et d'une compétence mondialement reconnues, s'est engagée résolument sur la voie de la cyber-résilience et aspire à transposer rapidement la directive NIS2, d'autres pays, moins avancés qu'elle, prêtent le flanc aux attaques malveillantes, exposant en même temps, par rebond, le cyberespace de leurs partenaires.

B. AUX MARCHES DE L'EUROPE : UN KALEIDOSCOPE GÉOPOLITIQUE

1. Bref panorama de la région

La région dite des Balkans occidentaux est constituée de six États : les cinq pays de l'ex-Yougoslavie n'ayant pas encore adhéré à l'Union Européenne, soit **le Monténégro, la Bosnie-Herzégovine, la Serbie, la Macédoine du Nord et le Kosovo, ainsi que l'Albanie** ; ils représentent au

---

[1] *L'ANSSI partage deux études de marché sur la cryptographie post-quantique menées auprès de l'écosystème, 25 novembre 2024.*

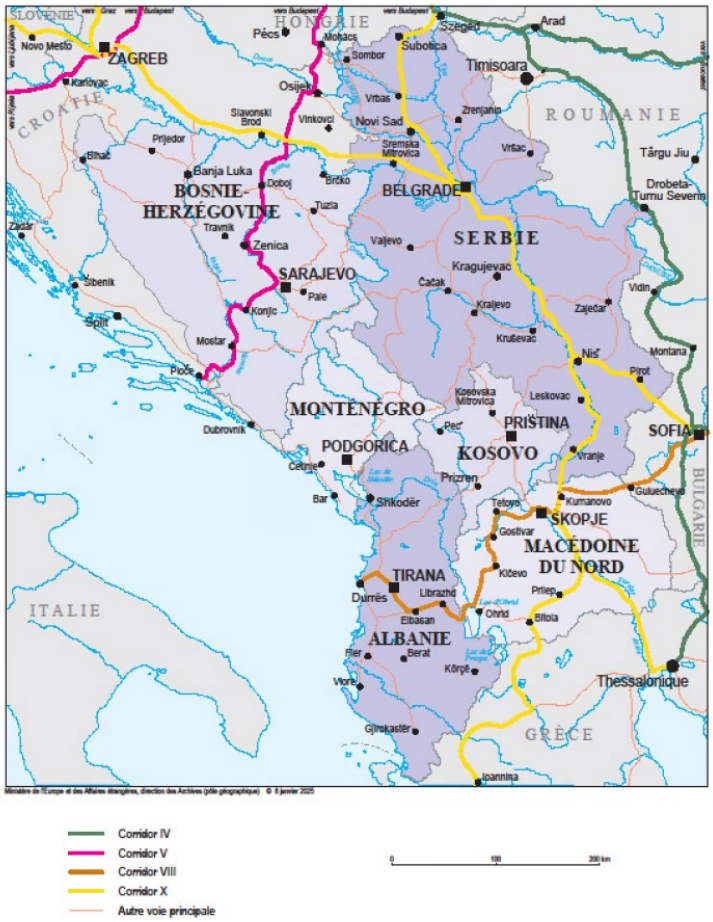
[2] *Soit la capacité d'une structure, d'un État à prévenir les incidents de cybersécurité, à y résister et à s'en relever.*

[3] *Source : indice relatif à la veille stratégique en matière de sécurité d'IBM.*

total, sur un peu plus de 200 000 km², environ 18 millions d'habitants – soit un peu plus que les Pays-Bas.

On souligna l'importance géostratégique de la région, traversée par trois des grands corridors paneuropéens :

BALKANS OCCIDENTAUX : CORRIDORS PANEUROPÉENS



Si l'économie de la région est d'ordinaire considérée comme « *saine dans l'ensemble* »[1], **la convergence économique avec l'Union européenne, qui demeure l'objet affiché, apparaît, à court et moyen terme, hors de portée** ; ainsi, la Banque européenne pour la reconstruction et le développement (BERD) estime **au minimum à 40 ans** le temps nécessaire aux Balkans occidentaux pour mener à terme le processus de convergence - dans l'hypothèse où son taux de croissance serait équivalent au taux moyen constaté sur la période 2001-2021[2].

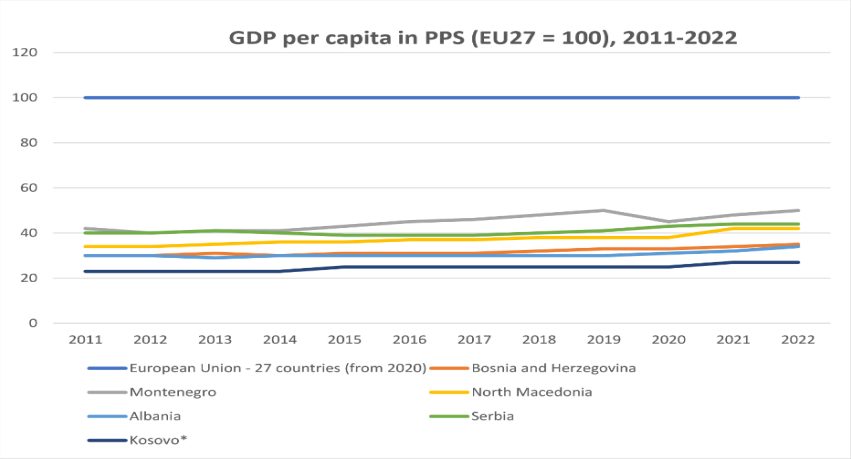
Le PIB par habitant, notamment, malgré des disparités entre pays, demeure très en deçà de la moyenne européenne :

---

[1] *Source : www.tresor.economie.gouv.fr.*

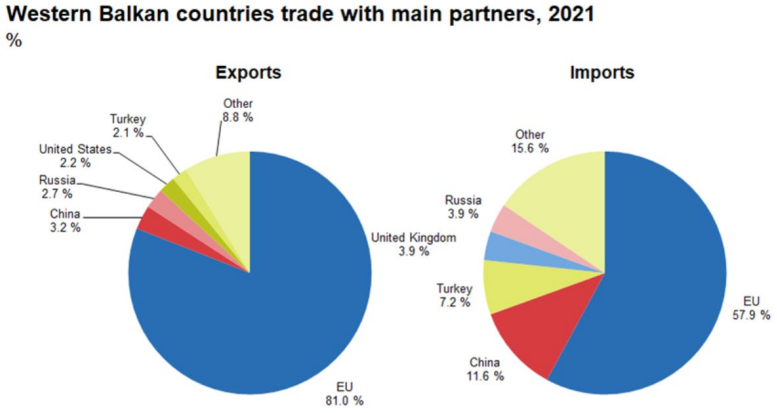
[2] *Les Balkans occidentaux peuvent-ils converger vers le niveau de vie de l'UE ?, février 2024.*

ÉVOLUTION DU PIB PAR HABITANT DES PAYS CANDIDATS DES BALKANS OCCIDENTAUX COMPARÉE À CELLE DU PIB PAR HABITANT DE L'UNION EUROPÉENNE ENTRE 2011 ET 2022



Source : Commission européenne, communication du 8 novembre 2023 sur le nouveau plan de croissance pour les Balkans occidentaux.

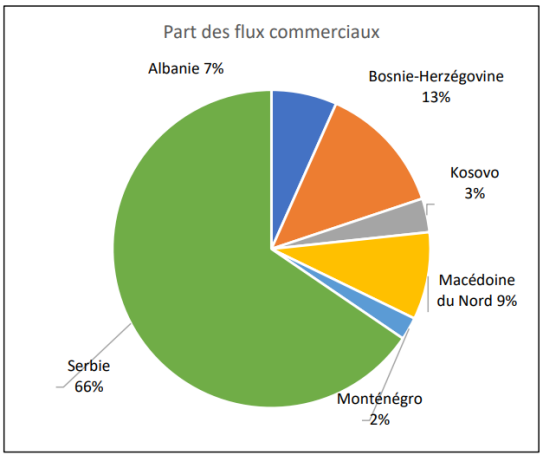
L'Union européenne demeure le principal partenaire commercial de la région, avec 81% des exportations et 57,9% des importations. La Russie, la Chine, la Turquie, notamment cherchent à développer leurs échanges.



Source: Eurostat (online data code: Comext data code : DS-056697)

Cependant inversement, **la part de la région dans le commerce global de l'Union européenne n'est que de 1,4 %, indice d'un partenariat commercial déséquilibré et insuffisant.**

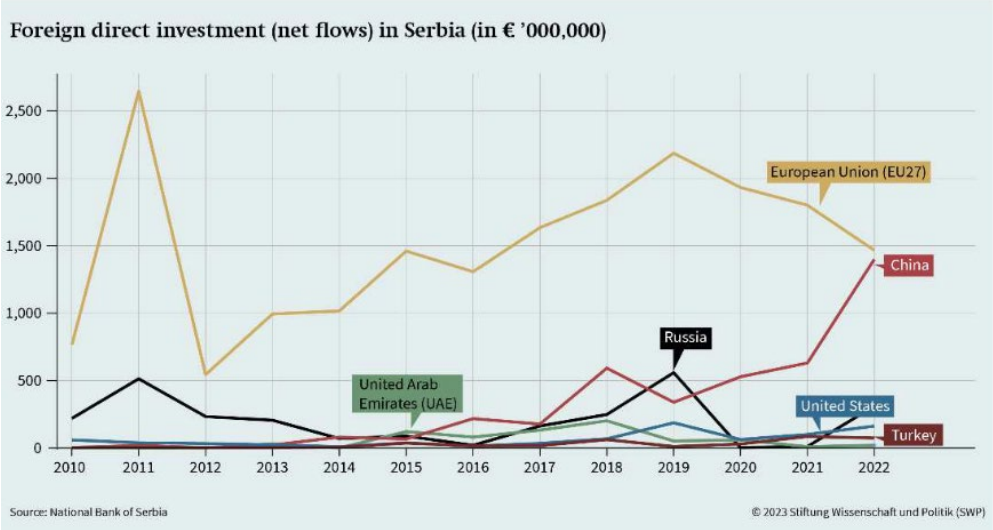
La France, quant à elle, est globalement peu impliquée dans ces échanges commerciaux, qui affichent cependant une progression constante (+146% entre 2014 et 2022). Son principal partenaire demeure la Serbie (66% des échanges) :



Source : www.tresor.economie.gouv.fr

S'agissant des investissements directs en provenance de l'Union européenne, ils s'élèvent pour la région à 17,021 Mds € en 2023.

En termes de flux cependant, on observe un essoufflement depuis 2019, contrairement aux investissements chinois qui suivent l'évolution inverse. À titre d'exemple, pour la Serbie, tous deux avoisinent aujourd'hui 1,5 Mds € (chiffre 2022).



Le stock d'investissements directs français dans la région représente quant à lui 544 millions € (dont 431 millions en Serbie, avec cependant un repli de 32% par rapport à 2019), soit à peine 2,5% des investissements européens.

En matière d'état de droit, ces pays, ayant souffert à des degrés divers des conflits des années 1990, ont engagé **une transition vers la démocratie, mais qui apparaît cependant inaboutie** : ils continuent à faire face, à des niveaux variables, à des défis importants en matière de consolidation de l'Etat de droit (indépendance de la justice, lutte contre la corruption et le crime organisé), de développement économique et social, ou encore de réconciliation et d'approfondissement de la coopération et de l'intégration régionale. Le classement *Freedom in the world*, de *Freedom House*, classe les six pays concernés dans la catégorie « *partly free* », sans évolution notable depuis

plusieurs années ; or les Acquis de l'Union européenne comportent plusieurs chapitres du bloc des « Fondamentaux » relatifs aux questions d'Etat de droit[1].

2. L'instabilité en héritage

La guerre entre républiques yougoslaves (1991-1995) a constitué le premier conflit d'envergure en Europe de l'après-guerre froide et a conduit à l'éclatement de l'ex-fédération yougoslave. Si l'affrontement direct a pris fin le 14 décembre 1995 avec les accords de Dayton, cette guerre laissait une région meurtrie, endeuillée de 100 000 morts, et profondément bouleversée du fait des quelque 2,4 millions de réfugiés et 2 millions de déplacés internes, qui ont bien souvent contribué à renforcer le clivage entre communautés et à pérenniser les tensions.

La guerre d'indépendance du Kosovo (1998-1999) est venue une seconde fois enflammer la région : la communauté albanaise du Kosovo, souhaitant s'affranchir de la domination serbe, constitua en 1996 l'Armée de libération du Kosovo (UÇK), déclenchant un nouvel affrontement qui entraînera l'intervention de l'aviation de l'OTAN, sans mandat onusien. C'est finalement en février 2008 que le Kosovo proclamera, unilatéralement, son indépendance, qui n'est toutefois pas reconnue à ce jour par un certain nombre de pays, dont cinq États membres de l'Union (Espagne, Grèce, Roumanie, Slovaquie et Chypre).

Ces deux conflits représentent des traumatismes originels qui ont profondément marqué la mémoire des populations régionales, et alimentent des contentieux non résolus.

La carte ci-après présente l'émiettement identitaire de la région :

Carte de l'Ex-Yougoslavie en 1999 © Studio graphique FMM

[1] *Dans une communication en date d'avril 2019, la Commission européenne a dégagé six principes constitutifs de l'État de droit qui sont : la séparation des pouvoirs ; les procédures législatives transparentes et démocratiques ; la sécurité juridique ; l'égalité en droit ; les juridictions indépendantes et impartiales ; l'efficacité du contrôle juridictionnel.*

3. Des tensions persistantes

Un quart de siècle après la fin des affrontements armés, plusieurs motifs de tensions, ouverts ou larvés, persistent, et constituent autant d'entraves à la progression de ces pays vers la normalisation de leurs relations :

En premier lieu **le différend entre la Serbie et le Kosovo n'a rien perdu de son intensité** : vingt-cinq ans après la fin des hostilités, la situation apparaît bloquée sur un *statu quo* à haut risque : la Serbie refusant de reconnaître le nouvel État, dont la sécurité demeure garantie par la présence de l'OTAN, tandis que la Russie soutient ouvertement les intérêts serbes, sur fond d'affrontements récurrents entre communautés[1].

S'agissant de **la situation en Bosnie-Herzégovine**, la Cour européenne des droits de l'homme s'est prononcée à six reprises contre la Bosnie-Herzégovine, du fait de sa constitution jugée discriminatoire envers certains groupes ethniques[2] (juifs et roms notamment) et de l'insuffisance démocratique des élections.

Des différends bilatéraux avec certains États membres voisins sont en outre susceptibles de peser sur le processus d'adhésion à l'Union européenne des pays des Balkans occidentaux : entre la **Bulgarie et la Macédoine du Nord**, concernant la reconnaissance du macédonien comme langue indépendante, entre la **Serbie et la Croatie,** marqué par le poids du passé**,** ou entre la **Grèce et l'Albanie**, qui semble cependant apaisé depuis la libération en septembre 2024 d'un personnalité politique d'origine grecque.

4. Les Balkans, carrefour d'influences

La situation des Balkans occidentaux, entre tensions et incertitude, les expose tout particulièrement aux manœuvres d'influence et aux ambitions régionales de puissances telles, notamment, la Chine, la Russie et la Turquie, désireuses d'asseoir par tous moyens leur emprise sur la région. Face à leurs diverses stratégies intrusives, le camp euro-atlantiste peine parfois à faire passer ses messages.

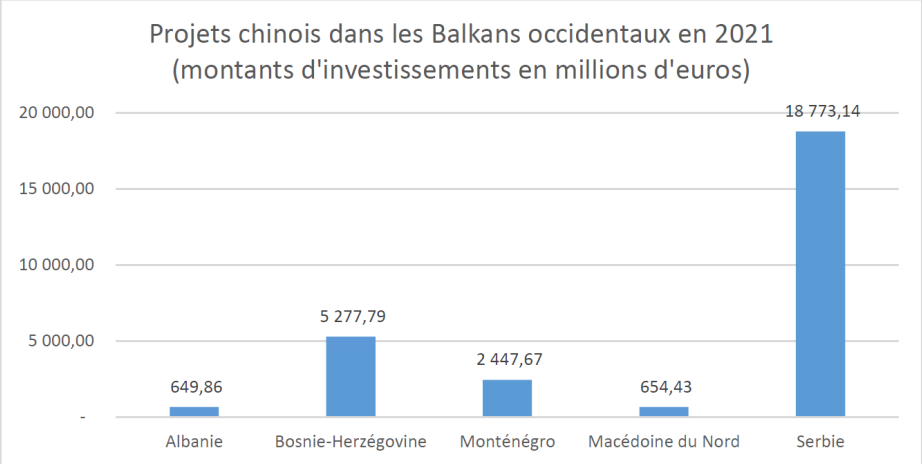
---

[1] *L'actualité récente a vu un regain de tension entre les deux pays, après le sabotage fin novembre d'un canal crucial pour l'approvisionnement en eau du Kosovo. Le Premier ministre kosovar, Albin Kurti, a aussitôt pointé du doigt le voisin serbe, qualifiant l'incident d'*« attaque terroriste » *et accusant la Serbie d'utiliser des « méthodes russes ».*

[2] *La constitution issue des accords de Dayton reconnaît trois peuples : les Bosniaques (musulmans), les Croates, les Serbes (catholiques et orthodoxes), pouvant être représentés dans la chambre haute, et deux territoires, celui des Bosniaques et des Croates, et celui des Serbes.*

➢ ***La Chine, une infiltration sur la durée des infrastructures stratégiques***

La Chine a identifié de longue date les Balkans occidentaux comme une porte d'entrée vers l'Union européenne, et y développe une stratégie de long terme, combinant des investissements ciblés soutenus par une « diplomatie de la dette » et d'aide au développement. **Elle a ainsi investi dans la région, entre 2009 et 2021, 32 milliards €, dont près d'un tiers en Serbie. Ces investissements représentent environ 40% des IDE dans la région** (hors Kosovo[1]).



Source : https://china.balkaninsight.com/

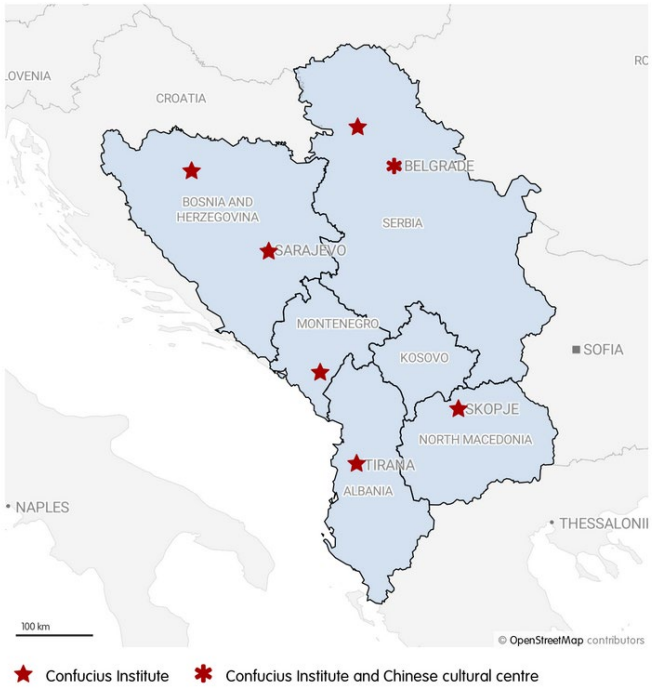
(Voir également graphique au B.1. ci-dessus)

Depuis 2014 et le lancement des « Nouvelles routes de la soie », la Chine se positionne progressivement comme une partenaire séduisante, offrant des financements rapides et des leviers concrets pour des projets volontiers pharaoniques, tels que l'autoroute Bar-Boljare au Monténégro, ou la ligne de chemin de fer rapide Belgrade-Budapest. Les financements chinois sont d'autant plus attractifs qu'ils ne s'accompagnent pas, comme les financements européens, de conditionnalités environnementales et sociales, ni en matière d'état de droit. Les investisseurs chinois ciblent de manière privilégiée les infrastructures mais aussi les secteurs énergétique et minier (industries d'extraction, centrales à charbon).

Il en résulte pour les pays de la région des niveaux d'endettement considérables, au point de menacer de compromettre la souveraineté économique des pays concernés. À titre d'exemple, la dette monténégrine vis à vis de la Chine atteint 20% de son PIB. En contrepartie des prêts accordés, la Chine impose souvent des clauses léonines, incluant parfois le droit de saisir des actifs stratégiques en cas de défaut de paiement.

Le *soft power* chinois est quant à lui très présent grâce notamment aux Instituts Confucius implantés dans la région :

[1] *La Chine ne reconnaît pas l'indépendance du Kosovo.*



Source : www.blue-europe.eu

La Chine apparaît ainsi « avancer ses pions » en vue d'une influence durable sur la région.

- ***La Russie et ses ingérences toxiques***

La Russie poursuit dans les Balkans occidentaux une stratégie d'influence dense et agressive, dans l'objectif affiché d'entraver tout nouvel élargissement de l'Union européenne et de l'OTAN dans la région.

Jouant de sa proximité avec certains cercles du pouvoir (armée, services de renseignement) et groupes nationalistes, mais aussi du relais de l'Église orthodoxe, elle cultive une image protectrice pour la communauté orthodoxe et porteuse d'une alternative au modèle occidental. L'influence de la Russie est notamment importante en Serbie et dans les zones de peuplement serbe (Republika Srpska en Bosnie-Herzégovine, Monténégro)[1].

Elle entretient un sentiment délétère vis-à-vis de l'enlisement du processus d'intégration (à l'heure actuelle, en Serbie, l'intégration européenne n'est plus souhaitée que par un tiers de la population), et joue un rôle important dans les tensions régionales (en Bosnie-Herzégovine ainsi qu'entre la Serbie et le Kosovo) qu'elle s'emploie à attiser.

Pour ce faire, elle utilise massivement tous les moyens de propagande, notamment cyber, développés au I.A. ci-dessus. Sa stratégie de désinformation s'appuie sur l'implantation de médias contrôlés par le pouvoir

[1] *Ce tropisme est hérité de la guerre du Kosovo, qui avait vu la Serbie visée par l'OTAN, tandis que la Russie lui apportait son soutien diplomatique.*

russe[1]. L'opinion serbe se montre particulièrement réceptive à cette propagande : à titre d'exemple, selon un sondage d'opinion réalisé en juin 2022 en Serbie, 54% des personnes interrogées estimaient que l'OTAN était le principal responsable de la guerre en Ukraine, contre 7% seulement qui en attribuaient la responsabilité à la Russie.

Les relations commerciales de la Russie avec la région sont quant à elles peu développées, à l'exception notable du secteur énergétique : La Russie fournit notamment à la Serbie 80 % du gaz consommé dans ce pays.

- ***La Turquie joue la carte de la proximité bienveillante***

Afin d'asseoir son influence sur les Balkans occidentaux, la Turquie tire profit de sa proximité géographique pour développer sa présence, notamment dans les pays où sont concentrées les principales communautés musulmanes - Albanie, Kosovo et Bosnie-Herzégovine.

Son *soft power* s'appuie notamment sur la construction de mosquées (240 dans le seul Kosovo ces 15 dernières années)[2], d'écoles et d'universités ; il joue également sur le financement de programmes de réhabilitation du patrimoine remontant à la période ottomane, sur la diffusion de séries télévisées populaires et sur le développement du réseau des **centres culturels *Yunus Emre*** (sur 23 centres culturels turcs dans le monde, 12 sont implantés dans les Balkans).

Sur le plan diplomatique, la Turquie œuvre en faveur de la pacification des relations interétatiques dans les Balkans et a notamment joué un rôle de médiateur en accueillant en 2010 un sommet à Istanbul, à l'issue duquel la Serbie et la Bosnie-Herzégovine ont signé une déclaration commune prévoyant l'intensification de leurs relations ainsi que la reconnaissance par la Serbie de l'intégrité territoriale de la Bosnie. Inversement, La Turquie peut trouver au sein de l'OTAN un appui auprès des trois membres balkaniques.

L'appartenance de la Turquie à l'Alliance et sa candidature à l'Union européenne ont d'autre part pour conséquence que le rapprochement avec la Turquie n'est pas perçu par les dirigeants des Balkans comme contradictoire avec une intégration euro-atlantique.

- ***Une implication volontariste du camp euro-atlantiste***

Face à ces pressions insistantes, l'Union européenne est loin de demeurer passive :

---

[1] *Citons notamment l'agence Spoutnik, qui dispose d'un bureau à Belgrade, ainsi que le média* « Russia Today » *(RT) qui dispose d'un canal de diffusion « RT Balkan ».*

[2] *Cette influence dans ce domaine se heurte néanmoins à celle de l'Arabie saoudite et du Qatar qui, depuis le début des années 1990, sont à l'origine de la construction de nombreuses mosquées et de l'envoi de prédicateurs fondamentalistes.*

La Stratégie pour les Balkans occidentaux, annoncée par le président de la Commission européenne Jean-Claude Juncker dans son discours sur l'état de l'Union de 2017, affiche pour objectifs de renforcer :

- L'état de droit : avec des plans d'action individuels consacrés à la mise en conformité avec les normes européennes, accompagnés de missions de conseil.
- La sécurité et le contrôle des migrations : avec une coopération renforcée dans la lutte contre le crime organisé, le terrorisme ou encore le renfoncement du contrôle des frontières.
- Le développement socio-économique : avec un ensemble de mécanismes destinés à faciliter le financement des PME, les programmes de réformes, la recherche et l'innovation.
- La connectivité en matière de transport et d'énergie : avec notamment une extension de l'Union de l'énergie aux Balkans occidentaux.
- La stratégie numérique : dans des domaines concrets tels que les coûts d'itinérance, le déploiement du haut débit, des services publics en ligne, etc.
- La réconciliation régionale et les relations de bon voisinage.

La stratégie expose également les mesures qui doivent être prises par le Monténégro et la Serbie pour compléter leurs processus d'adhésion avec l'objectif de remplir les critères de Copenhague d'ici à 2025.

L'Union européenne a adopté en 2023 un plan de croissance destiné à permettre aux pays de la région d'accélérer les réformes avec une nouvelle **facilité pour la réforme et la croissance de 6 milliards d'euros** pour la période 2024-2027.

La France s'investit tout particulièrement dans son rapprochement avec la région, avec sa **Stratégie interministérielle pour les Balkans occidentaux**, décidée en 2019, qui renforce sa coopération bilatérale avec les pays de la région dans cinq domaines :

- Présence et influence économique, notamment avec l'intervention de l'Agence française de développement (AFD) ;
- Sécurité[1] ;
- Défense ;
- Justice ;
- Culture, éducation, langue française et jeunesse.

[1] *Notamment la lutte contre les trafics illicites d'armes légères et de petit calibre.*

Elle œuvre auprès des pays de la région à compléter l'action de l'Union européenne pour soutenir leur rapprochement européen et, globalement, à intensifier ses relations politiques avec eux.

La création du C3BO faisant l'objet du présent rapport s'inscrit dans ce cadre.

De son côté l'OTAN maintient, conformément à la résolution 1244 adoptée le 10 juin 1999 par le Conseil de sécurité de l'ONU, un effectif de 4 500 personnels au Kosovo, dans le cadre de la KFOR, afin de maintenir un environnement sûr et de préserver la liberté de circulation au sein du petit pays.

Une compétition d'influence majeure est en train de se jouer dans la région des Balkans occidentaux, véritable course contre la montre dans le contexte de sa potentielle intégration européenne. L'Europe, et notamment la France, doivent en prendre toute la mesure, afin d'éviter des évolutions qui pourraient mettre en péril la stabilité de la région. Comme le soulignait le chancelier Olaf Scholz [1]: « *Les six pays des Balkans occidentaux font partie de la famille européenne. Leur avenir est dans l'Union européenne … Il est grand temps de passer des paroles aux actes* ».

C. QUELLE INTÉGRATION POUR LES BALKANS ?

1. Le long chemin vers l'Union européenne

Les six pays constituant les Balkans occidentaux aspirent globalement, et de longue date, à intégrer l'Union européenne. Mais, 22 ans après le sommet de Thessalonique des 19 et 20 juin 2003 qui avait affirmé une « *perspective européenne des pays des Balkans occidentaux* »[2], force est pour eux de constater que l'Union européenne ne s'est pas montrée à la hauteur des espoirs qu'elle a suscité.

Le processus d'adhésion, laborieusement entamé, se voit, pour chacun d'eux à des degrés divers, contrarié par une succession de blocages (voir ci-après), **qui viennent freiner ou entraver son avancement.**

[1] *Conférence de presse tenue le 14 octobre 2024.*
[2] *v. conclusions du Conseil européen de Thessalonique des 19 et 20 juin 2003, §40*

Etat membre Candidat officiel Candidature déposée

Source : www.touteleurope.eu

Le rapport d'information sénatorial de M. Olivier Cigolotti, Mme Hélène Conway-Mouret, M. Bernard Fournier, et Mme Michelle Gréaume[1] pointait les conséquences délétères de ces atermoiements, en soulignant que « *Vingt ans après le sommet de Thessalonique, la lenteur du processus d'intégration nuit à la crédibilité de l'Union européenne dans les Balkans occidentaux* » ; et craignait que « *L'inaboutissement du processus d'intégration européenne des Balkans favorise un investissement croissant des puissances extérieures dans la région* ».

En Serbie notamment, la lenteur du processus a suscité auprès de l'opinion un sentiment de frustration voire de découragement : En 2009, 73% des Serbes étaient favorables à l'adhésion, contre seulement 34% actuellement.

Ce ressenti trouve confirmation dans la célérité avec laquelle le statut de candidat a été octroyé à l'Ukraine et à la Moldavie en juin 2022 dans le sillage du déclenchement de la guerre en Ukraine, après que la Slovénie, en 2004, et la Croatie, en 2013, aient été les deux seuls pays de la région à avoir mené à son terme leur processus d'adhésion.

[1] *Réinvestir les Balkans occidentaux : un impératif stratégique, rapport d'information n°882 (2022-2023).*

Dans le détail :

Le **Monténégro** a déposé sa demande d'adhésion en décembre 2008 et commencé les négociations d'adhésion en juin 2012 : il est actuellement le **candidat le plus avancé sur la voie de l'intégration européenne**, avec 33 chapitres de négociation ouverts, dont trois provisoirement clos, et espère clore plusieurs autres chapitres prochainement. Il est notamment le seul candidat à remplir les critères intermédiaires fixés sur les chapitres 23 et 24 relatifs à l'état de droit.

La **Serbie**, qui a déposé sa demande d'adhésion en décembre 2009 et commencé les négociations d'adhésion en janvier 2014, a ouvert 22 chapitres de négociation, dont deux provisoirement clos, puis un nouveau bloc de chapitres en décembre 2021 (bloc n°4 sur l'agenda vert et la connectivité durable). Depuis 2021, le bloc n°3 sur la compétitivité et la croissance inclusive est « techniquement prêt » à être ouvert**. Cependant, plusieurs États membres s'opposent à l'ouverture de tout nouveau bloc**, en raison du faible taux d'alignement de la Serbie sur la PESC (58% en 2024), et notamment son défaut d'alignement sur les sanctions contre la Russie.

La **Macédoine du Nord** a déposé sa demande d'adhésion dès mars 2004. Les progrès de sa candidature ont connu des difficultés en raison de différends bilatéraux, d'abord avec la Grèce, (réglé en 2020 avec l'Accord de Prespa[1]), puis avec la Bulgarie (qui a fait l'objet d'un compromis négocié par la France à la fin de la Présidence française de l'Union européenne en 2022). La poursuite du chemin européen de la Macédoine du Nord est désormais **conditionnée à la mise en œuvre d'une réforme constitutionnelle permettant la reconnaissance d'une minorité bulgare**.

L'**Albanie** a déposé sa demande d'adhésion en avril 2009 et a obtenu l'accord du Conseil européen sur l'ouverture de négociations d'adhésion en mars 2020. Cependant, en raison du différend bulgaro-macédonien, le cadre de négociation n'a été adopté qu'en juillet 2022. L'ouverture du **premier bloc de chapitres, celui des fondamentaux, en octobre 2024**, a dû attendre la levée des réserves de la Grèce après la libération d'une personnalité politique d'origine grecque. L'Albanie pourrait voir l'ouverture du bloc n°6 sur les relations extérieures prochainement.

La **Bosnie-Herzégovine**, qui a déposé sa demande d'adhésion en février 2016, s'est vue accorder le statut de pays candidat en décembre 2022. Le Conseil européen de mars 2024 a décidé d'ouvrir les négociations d'adhésion et **conditionné l'adoption du cadre de négociation à huit mesures** liées au statut de pays candidat (portant notamment sur la réforme de la justice, l'État de droit, la lutte contre la corruption et la criminalité organisée,

[1] *L'accord de Prespa, conclu le 11 juin 2018 entre la Grèce et la république de Macédoine, prévoit notamment le remplacement du nom provisoire de l'ancienne république yougoslave de Macédoine, par le nouveau nom de « république de Macédoine du Nord ».*

la gestion des frontières et des migrations et la reprise de l'acquis de l'Union européenne).

Le **Kosovo** a quant à lui déposé sa demande d'adhésion en décembre 2022, mais **l'avancée de son chemin européen se heurte notamment au fait que cinq États membres** (Chypre, Espagne, Grèce, Roumanie et Slovaquie) **ne le reconnaissent pas**. Le rapprochement européen du pays s'inscrit dans une démarche plus large du Kosovo, qui cherche également à se rapprocher de l'OTAN, à consolider sa souveraineté et à renforcer la reconnaissance internationale de son indépendance.

Cependant, il apparait que l'invasion russe de l'Ukraine en février 2022 soit soudain venue redynamiser le processus d'adhésion de ces pays qui semblait grippé, faisant « *prendre conscience à l'UE* », comme l'écrit Appoline Carras, « *de l'importance stratégique de l'élargissement et du besoin crucial de l'unité face aux volontés impérialistes du Kremlin* »[1]. De fait, récemment, le contenu des sommets consacrés aux Balkans occidentaux semble se densifier et le dialogue donner des signes tangibles de progression.

Le rapport d'information publié par l'Assemblée nationale sur l'évolution des négociations d'adhésion entre les pays des Balkans occidentaux et l'Union européenne[2] y insiste : « *L'élargissement de l'Union aux pays des Balkans est une perspective inéluctable. La guerre en Ukraine crée en effet une situation nouvelle en Europe qui interdit à l'Union de rester confinée dans son périmètre actuel. Par ailleurs, il est peu envisageable de ne pas faire adhérer des pays avec lesquels l'Union négocie pour certains (Serbie, Monténégro) depuis plus de dix ans. En leur fermant la porte, l'Union perdrait sa crédibilité et créerait un risque grave de déstabilisation dans une région située à sa périphérie immédiate. L'Union européenne et les États membres n'ont pas d'autre choix que de mobiliser tous les instruments dont ils disposent, au niveau multilatéral comme bilatéral, pour accompagner ces pays dans les réformes indispensables à leur future adhésion*. ».

Dans son discours de clôture du forum GLOBSEC de Bratislava, le 31 mai 2023, le président Macron indiquait : « (…) *la question pour nous n'est pas de savoir si nous devons élargir, nous y avons répondu il y a un an ; ni même quand nous devons le faire, c'est pour moi le plus vite possible, mais bien comment nous devons le faire* ».

2. Une orientation résolument atlantiste

Avec un processus d'adhésion plus inclusif que celui de l'Union européenne, l'OTAN a d'ores et déjà arrimé au bloc atlantiste, à différents degrés, les pays de la région :

---

1 Balkans occidentaux. Dans l'antichambre de l'Union européenne ? Diploweb.com, 12 janvier 2025.

2 Rapport d'information n° 2467 du 10 avril 2024, par M Pierre-Henri Dumont et Mme Liliana Tanguy.

L'Albanie, le Monténégro et la Macédoine du Nord ont rejoint l'Alliance respectivement en 2009, 2017 et 2020 : L'élargissement à l'Albanie a apporté à l'Organisation un premier ancrage solide dans les Balkans occidentaux. L'élargissement au Monténégro s'est fait dans un contexte compliqué (tentative de coup D'état au moment où celui-ci s'apprêtait à la rejoindre). La Macédoine du Nord est le dernier État des Balkans occidentaux à avoir rejoint l'OTAN, après avoir résolu son différend avec la Grèce par l'accord de Prespa.

La Bosnie-Herzégovine est actuellement engagée dans un processus pour rejoindre l'Alliance. A cette fin, en 2019, la Bosnie-Herzégovine, dans le cadre de son Plan d'action pour l'adhésion (MAP), a présenté son premier programme de réformes, qui décrit les réformes que le gouvernement s'engage à entreprendre ainsi que l'aide apportée par l'OTAN à ces efforts. Par ailleurs, début 2021, la Bosnie-Herzégovine a créé la Commission pour la coopération avec l'OTAN, qui coordonne la mise en œuvre de ce programme de réformes. Cependant, le rapprochement avec l'OTAN n'est pas consensuel, les Bosno-serbes plaidant en faveur d'une neutralité militaire, à l'instar de la Serbie.

La Serbie a proclamé en 2007 sa neutralité militaire. Cette prise de distance avec l'Alliance tire son origine des frappes aériennes infligées par l'OTAN à des cibles serbes, en 1999, lors de la guerre du Kosovo. Le pays entretient cependant un dialogue constructif avec l'OTAN depuis le Partenariat pour la paix signé en 2006 ; en janvier 2015, la Serbie et l'OTAN ont conclu un plan d'action de partenariat individuel (reconduit en novembre 2019), qui exclut toute future adhésion à l'Alliance mais renforce la coopération entre les deux parties. Le Kosovo demeure un élément-clé de ce partenariat du fait de la participation de la Serbie à la KFOR, déployée sous la direction de l'OTAN pour maintenir un environnement sûr et sécurisé au Kosovo, en application de la résolution 1244 du Conseil de sécurité des Nations unies.

Le Kosovo brigue une adhésion à l'OTAN, et a conclu dans ce sens un partenariat pour la paix. Les efforts de Pristina se heurtent toutefois à la règle de l'unanimité pour les décisions d'adhésion de nouveaux membres à l'Alliance, alors que plusieurs de ses membres ne reconnaissant pas l'indépendance du Kosovo.

3. Synthèse : une intégration à plusieurs vitesses :

	Union Européenne			OTAN	
	Année de demande	Avancement	Commentaires	Avancement	Commentaires
Monténégro	2008	Bien avancé	33 chapitres de négociation ouverts, dont trois clos, et plusieurs en cours de clôture.	Membre depuis 2017	
Serbie	2009	Assez avancé, mais blocage	22 chapitres de négociations ouverts dont deux clos. Plusieurs États membres s'opposent à l'ouverture de tout nouveau bloc, en raison du faible taux d'alignement de la Serbie sur la PESC.	Neutralité militaire	Adhésion au Partenariat pour la paix de l'OTAN en 2006. Signature avec l'OTAN en 2015 d'un plan d'action de partenariat individuel.
Macédoine du Nord	2004	Peu avancé	Progrès difficiles en raison des différends bilatéraux, d'abord avec la Grèce, puis avec la Bulgarie. Actuellement en attente d'une réforme constitutionnelle reconnaissant la minorité bulgare.	Membre depuis 2020	
Albanie	2009	Peu avancé	Premier bloc de chapitres ouvert en 2024 (fondamentaux). Un autre bloc pourrait être prochainement ouvert.	Membre depuis 2009	
Bosnie-Herzegovine	2016	Peu avancé	Adoption du cadre de négociation conditionné à plusieurs réformes préalables	Procédure d'adhésion en cours	Plan d'action pour l'adhésion (MAP) en 2015. Commission pour la coopération avec l'OTAN en 2021.

Kosovo	2022	Blocage	Blocage du fait que cinq États membres ne le reconnaissent pas. N'a pas encore obtenu le statut de candidat.	Souhait d'adhésion mais blocage	Blocage du fait que plusieurs États membres ne le reconnaissent pas.

D. LES BALKANS OCCIDENTAUX, MAILLON FAIBLE DE LA CYBERSÉCURITÉ EUROPÉENNE

1. Des défenses sous-dimensionnées…

Le niveau de préparation des pays balkaniques face à la menace cyber est inégal, même si les cyberattaques de 2022 et 2023 ont entraîné une prise de conscience. Ainsi, au regard de la directive NIS2 :

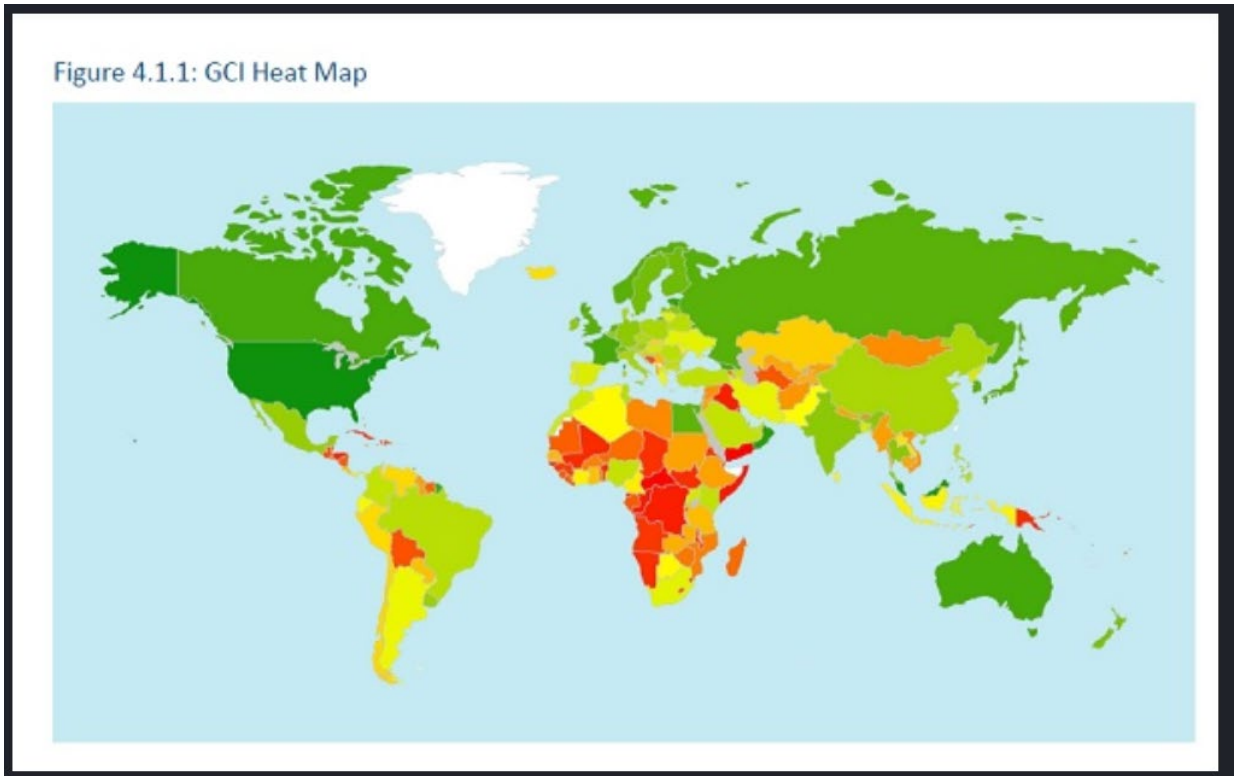
- La Serbie a renforcé son cadre réglementaire, avec l'adoption dès 2015 d'une loi sur la cybersécurité. Elle travaille actuellement à s'aligner sur la directive NIS2.
- L'Albanie a considérablement amélioré sa cyber résilience suite aux attaques de 2022. Elle dispose aujourd'hui de moyens de formation et de capacités propres, et travaille à s'aligner sur NIS2.
- Le Monténégro est sur le point de se doter d'une loi sur la cybersécurité, et a annoncé la création d'une agence nationale de cybersécurité courant 2025.
- Le Kosovo travaille à l'élaboration d'une stratégie cyber et d'une loi afférente. Le premier directeur de l'autorité cyber a été nommé en octobre 2024.
- La Macédoine du Nord ambitionne de transposer NIS2 dans les deux prochaines années.
- La Bosnie-Herzégovine apparaît la moins avancée (absence de stratégie nationale, peu de capacités techniques, absence de CSIRT national, pas de projet de loi visant à s'aligner sur la directiveNIS2…). Son morcellement administratif rend ce pays particulièrement vulnérable.

Globalement, la vulnérabilité des pays des Balkans occidentaux tient à des difficultés de coordination institutionnelle et à une prise de conscience politique inégale de la menace cyber. Le phénomène de saut technologique, qui a vu les administrations balkaniques tenter une numérisation rapide sans prise en compte de la cybersécurité, combiné à la faiblesse de la protection

initiale et au manque de culture de sécurité, explique également la vulnérabilité de la région.

En termes de moyens humains, des difficultés de recrutement et de fidélisation des compétences techniques-clés facilitent le succès des cyberattaques, dans un contexte de crise démographique et de fuite des cerveaux touchant tout particulièrement le domaine des nouvelles technologies. L'absence d'écosystème, notamment privé, de cybersécurité, fait peser en outre un risque de valorisation criminelle sur les quelques spécialistes disponibles sur le marché[1]. Il en résulte dans l'ensemble de la région un niveau insuffisant de compétences qui représente un obstacle majeur à sa résilience cyber et entraîne trop souvent le développement de pratiques irresponsables.

Le *Global security index* classe ainsi les Balkans occidentaux parmi les zones les plus vulnérables de la planète :



Source : Global Security Index, Organisation des Nations unies

[1] *Ainsi,* Cytrox AD, *filiale de la galaxie* Intellexa *basée en Macédoine du Nord, a joué un rôle-clé dans la production du logiciel espion hautement intrusif* Predator. Cytrox AD *a été ajoutée sur* l'Entity List *du Département du Commerce américain le 18 juillet 2023 pour avoir vendu des exploits utilisés pour obtenir des accès à des systèmes d'information, et sur la liste des désignations de l'OFAC du Département du Trésor le 5 mars 2024.*

2. …faisant de ces pays des cibles faciles…

L'Albanie, puis le Monténégro, ont souffert à l'été 2022 d'une série de cyberattaques sans précédent dans la région par leur ampleur, faisant la preuve, s'il en était besoin, de la capacité de nuisance de leurs agresseurs.

- Le 15 juillet 2022, l'Albanie a été victime d'une cyberattaque d'ampleur et sophistiquée, ayant touché des infrastructures et de systèmes gouvernementaux. Les attaquants auraient réussi à infiltrer des réseaux gouvernementaux et à exfiltrer des données en amont du 15 juillet, avant de déployer un rançongiciel (chiffrement de données) et un *wiper* (destruction de données). Le 10 septembre 2022, la police albanaise a subi une nouvelle cyberattaque qui a temporairement mis hors ligne son *Total Information Management System* (TIMS), un système informatique de contrôle des arrivées et des départs utilisés par les douanes albanaises. Les autorités albanaises, ainsi que les Etats-Unis et Microsoft, ont publiquement attribué la cyberattaque à la République Islamique d'Iran. Tirana considère que ces cyberattaques étaient des mesures de rétorsion de l'Iran suite à l'accueil sur le territoire albanais de membres de l'organisation des moudjahidines du peuple iranien (OMPI).
- Le 22, puis le 26 août 2022, les autorités monténégrines ont annoncé qu'une cyberattaque d'ampleur affectait plusieurs de leurs institutions publiques. Cette cyberattaque est intervenue dans le contexte de la guerre d'agression de la Russie contre l'Ukraine, plusieurs mois après que le Monténégro a été placé sur la liste des « pays ennemis » de la Russie. L'ampleur de l'attaque a conduit le Premier ministre à demander l'aide de ses partenaires internationaux. Répondant à cet appel, la France a déployé temporairement sur place une équipe de réponse à incident cyber de l'ANSSI.

Les pays des Balkans occidentaux continuent à être fréquemment visés par des cyberattaques. Ainsi, l'Albanie a indiqué en décembre 2023 que le site du Parlement avait été ciblé, puis début février 2024 que son institut national des statistiques avait été victime d'une cyberattaque sophistiquée.

3. …et créant des vulnérabilités pour ses partenaires

Dans un espace de conflictualité hybride, en partie immatériel, et où les attaquants se jouent des frontières, le renforcement de notre résilience nationale ne peut être pleinement efficace sans un renforcement des capacités cyber plus global : La Revue nationale stratégique du 9 novembre 2022 soulignait ainsi 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 cyberespace dans son ensemble. ».

Cette fragilité de l'espace cyber des Balkans occidentaux, au vu des risques de rebond, constitue une menace majeure pour les réseaux et infrastructures cyber des États membres de l'Union européenne ainsi que des Alliés de l'OTAN. Dans la perspective d'un aboutissement, à moyen terme, des processus d'intégration en cours, une mise à niveau de leurs capacités de résilience cyber est indispensable, faute d'apporter des failles de sécurité chez l'ensemble de leurs partenaires.

Dans ce contexte, le soutien apporté au développement des capacités cyber de la région des Balkans occidentaux prend tout son sens, et la France a tout particulièrement un rôle à y jouer :« *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* » estimait la Revue stratégique de cyberdéfense de la France de février 2018.

II. LE PROJET D'ACCORD PORTANT CRÉATION DU CENTRE DE DÉVELOPPEMENT DES CAPACITÉS CYBER DANS LES BALKANS OCCIDENTAUX (« C3BO »)

A. LA GENÈSE DE L'ACCORD, OU LA DÉMARCHE VOLONTARISTE DES TROIS MEMBRES FONDATEURS

L'accord a fait l'objet d'une relative célérité dans son élaboration et sa maturation, au regard des délais habituels nécessaires aux processus de ratification des conventions internationales. Cette diligence est essentiellement motivée par **l'urgence à pallier une faille -sécuritaire majeure au sein du cyberespace européen**.

1. Premier trimestre 2022 : la mission de préfiguration franco-slovène

De janvier à avril 2022, une mission de préfiguration conduite par la France et la Slovénie a dressé le constat, à l'issue de nombreux entretiens avec des experts régionaux, que les pays des Balkans occidentaux étaient inégalement avancés en matière de cybersécurité, du fait notamment d'un manque de main d'œuvre qualifiée ; la mission a préconisé un renforcement de la coopération avec la région de manière à partager les informations et bonnes pratiques dans ce domaine. La création d'un Centre dédié au partage de capacités cyber est apparu comme une réponse adéquate, et l'ensemble des pays des Balkans occidentaux a très vite manifesté le souhait d'adhérer à ce projet.

2. Le choix du Monténégro comme pays hôte

Si tous les pays bénéficiaires de l'accord ont déclaré leur candidature pour héberger le centre, l'offre du Monténégro est apparue à la France et à son partenaire slovène comme la mieux motivée et la plus cohérente, dans un contexte où ce pays était le plus avancé dans le processus d'intégration à l'Union européenne.

3. L'aboutissement du projet

Dès novembre 2022 est signée par les trois membres fondateurs (France, Slovénie, Monténégro) une lettre d'intention tripartite, prédéfinissant le cadre et les orientations de la future coopération. Il est notamment prévu que la future organisation internationale permette, dès l'entrée en vigueur de l'accord, aux autres pays des Balkans occidentaux de devenir membres de droit de la structure ; le projet prévoit que d'autres pays pourront également adhérer, anticipant ainsi le développement à venir du Centre.

Les travaux du Centre ont débuté au printemps 2023, avec une première formation délivrée à compter du 8 mai 2023 ; d'autres sessions de formation ont suivi, comme notamment « *Her CyberTracks Europe Forum* », le 18 septembre 2023.

L'accord a été signé le 23 octobre 2023 par les trois membres fondateurs, dans le cadre d'un sommet consacré au « processus de Berlin ».

B. LE C3BO AU SERVICE DE LA RÉSILIENCE CYBER

Dénommé Centre de développement des capacités cyber dans les Balkans occidentaux ou « C3BO » (WB3C), le centre délivre des **formations à la cybersécurité, la lutte contre la cybercriminalité et la promotion de la cyberdiplomatie** et du partage des bonnes pratiques, permettant ainsi de renforcer les écosystèmes cyber des pays de la région. Destiné tant aux services de police qu'aux magistrats, aux administrations et aux entreprises du secteur privé, il vise non seulement un renforcement mais surtout une structuration des capacités cyber (développement d'instruments de formation, mise à disposition d'équipements, formation de spécialistes en lutte contre la cybercriminalité). Il contribue également à soutenir le renforcement du cadre réglementaire des pays de la région de façon à garantir un niveau d'exigence de résilience cyber élevé, en accord avec les standards de l'Union européenne.

La création du C3BO est originale à plusieurs titres :

- **Par sa dimension régionale** : il constitue en effet la première structure cyber *ad hoc* établie dans la région, développant une coopération technique à l'échelle régionale essentielle pour répondre efficacement aux

menaces et renforcer la résilience cyber ; il prévoit notamment la participation d'experts régionaux qui contribueront à l'encadrement des formations, aux côtés des experts français et slovènes -ce qui constitue une autre particularité par rapport aux autres écoles nationales à vocation régionales (ENVR) existantes ;

- **Par son caractère pérenne** : il n'existait antérieurement que des formations ponctuelles dans le domaine cyber ;

- **Par son format juridique** : Le C3BO est également la seule ENVR à être développée dans le pays hôte (Monténégro) en partenariat avec un État tiers (Slovénie), et à briguer le statut d'organisation internationale ;

- **Par le contenu de son enseignement** : Les enseignements dispensés au C3BO sont essentiellement d'ordre pratique et impliquent la mise à disposition d'équipements et de solutions logicielles, avec une attention toute particulière portée à la dimension pédagogique.

Depuis la signature, le 16 novembre 2022, d'un Mémorandum entre la France, la Slovénie et le Monténégro, État hôte, le projet C3BO s'est matérialisé avec le démarrage des actions de formation dès mai 2023, dans les locaux de l'Université du Monténégro, dans l'attente de la remise de ses locaux définitifs.

Ceux-ci ont été livrés par le Monténégro, au sein du nouveau Parc scientifique et technologique de Podgorica, en juin 2024, à l'occasion d'une conférence cyber régionale organisée par le Centre.

En 2023, cinq formations ont ainsi été organisées par le C3BO au profit des académies de police, de magistrats et de responsables de la sécurité des systèmes d'information (RSSI) de la région, et un événement de sensibilisation en direction des femmes décideurs politiques aux questions cyber (en partenariat avec la GIZ) a été organisé. **En 2024, 400 stagiaires ont suivi 21 formations**. Pour ces premières formations de haut niveau (60% dans le domaine de la lutte contre la cybercriminalité, 30% en cybersécurité, 10% en cyberdiplomatie), le ComCyberMI français, la Réserve cyber de la gendarmerie nationale, ainsi que le secteur privé (Total, HarfangLab…) ont été mis à contribution. **Pour 2025, 31 formations visant 600 stagiaires sont prévues**.

L'enseignement est dispensé en langue anglaise ; aucune langue de travail n'est définie pour le fonctionnement du Centre en lui-même, implanté en territoire monténégrin, les formateurs étant pour l'essentiels français, et le personnel administratif slovène.

Ces formations sont dispensées **à titre entièrement gratuit** pour les bénéficiaires, prenant en charge leurs frais de transport, de logement et de séjour.

La commission a cependant jugé, dans le contexte budgétaire actuel, ces modalités de prise en charge excessivement généreuses, et a estimé que les formations pourraient être conditionnées à une participation financière, au moins symbolique, des bénéficiaires. Elle a émis une recommandation dans ce sens.

C. IMPACT ET ENJEUX DE L'ACCORD

1. Le coût du projet

La France s'est investie financièrement dans le projet depuis 2022, avec des crédits à hauteur de 165 000 € (dont 50 000 € inscrits au titre 2 : dépenses de personnel). En 2023, les crédits, accompagnant la montée en puissance du centre[1], se sont élevés à 450 000 € (dont 265 000 € en titre 2) et en **2024 ils ont atteint 870 000 €** (dont 440 000 € en titre 2)[2]. La contribution française devrait se maintenir à ce niveau, au moins à court terme.

Ces fonds sont imputés au programme budgétaire 105 « Action de la France en Europe et dans le Monde ».

La France déploie aujourd'hui sur ce projet trois coopérants français (deux militaires de la gendarmerie et un expert technique international de la police nationale). Le directeur des études doit être relevé au 1er janvier 2025 par un officier supérieur de gendarmerie.

Le Monténégro participe à hauteur de 80 000 € annuels *via* la location de l'emprise où est située le C3BO. Cette contribution devrait légèrement augmenter avec la prise à bail de salles supplémentaires.

La Slovénie quant à elle prend en charge les salaires des trois recrutées locales pour un montant total d'environ 100 000 € par an. Cet investissement augmentera avec le financement, annoncé par la Slovénie, d'un expert en charge de couvrir le volet « cybersécurité » du Centre.

Contrepartie du rôle pilote joué par la France, celle-ci contribue ainsi actuellement à hauteur de 83% du financement du centre.

A cet égard, la transformation du C3BO en organisation internationale aura un impact sur le coût global du centre, mais aussi sur la répartition des contributions :

---

[1] *Cette augmentation s'explique par le fait que le Centre est passé de quelques formations en 2023 à 21 en 2024, et de 50 stagiaires à plus de 400. De même, l'unique coopérant a été rejoint par deux autres.*

[2] *Ces chiffres sont sensiblement différents de ceux figurant dans l'exposé des motifs du projet de loi, qui indique «* Ces fonds s'élèvent à 524 000 euros en 2023 et 1 172 000 euros en 2024 » *; l'écart s'explique par le fait que, ce montant a été estimé au début du processus de ratification. Or entretemps le coopérant responsable du C3BO et directeur des études a démissionné de manière inattendue et sa relève n'est pas intervenue avant la fin de l'exercice 2024 (pas de traitement versé en 2024). »*

La transformation du Centre devrait entraîner une augmentation de la masse salariale, et donc de son coût, difficilement quantifiable à ce stade. Elle permettra cependant, à l'inverse, une participation financière de la part des États bénéficiaires et de possibles nouveaux membres.

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

La commission a estimé que, dans le contexte budgétaire actuel, il conviendrait de tendre, pour l'avenir et au fur et à mesure que l'organisation internationale s'enrichira de nouveaux membres, vers une répartition moins déséquilibrée des contributions financières entre les membres, et a émis une recommandation dans ce sens.

2. Les bénéfices attendus

Pour la diplomatie française, l'enjeu du C3BO est triple :

Tout d'abord, bien sûr, il **présente un enjeu de cybersécurité, pour la région, mais aussi pour ses partenaires français, européens et atlantistes**. A cet égard, l'enjeu de formation est majeur, du fait de l'insuffisance de compétences dont souffre la région dans ce domaine. Du fait de leur médiocre culture de la cybersécurité, les pays des Balkans occidentaux sont en effet particulièrement vulnérables, comme détaillé 1D ci-dessus : on l'a vu avec l'offensive perpétrée par la Russie contre le Monténégro, en 2022, en raison de sa position face au conflit ukrainien, et celle lancée par l'Iran à l'encontre de l'Albanie, la même année, en représailles à l'hospitalité accordée aux moudjahidines du peuple.

Or il en va de l'intérêt général, et notamment de celui de l'Union européenne et donc de la France, de voir renforcer la cyber-résilience de nos partenaires, afin d'éviter toute compromission par rebond de notre propre cyberespace. Cette même problématique se pose avec une acuité particulière dans le cadre de l'OTAN, et explique que, en même temps que la France et la Slovénie, les Etats-Unis se préoccupent de la cybersécurité des Balkans occidentaux au point d'installer également au Monténégro un centre cyber, doté de missions complémentaires à celles du C3BO[1].

En second lieu, la région des Balkans occidentaux constitue un enjeu géostratégique majeur : dans un contexte où le processus d'adhésion à l'Union européenne est pour ces pays particulièrement lent, ou en panne, leur enthousiasme pro-européen tend à s'émousser et ouvre la brèche à un réel

[1] *Voir « Washington paré pour supplanter Paris dans le cyber balkanique », Intelligence on line, 25 novembre 2024.*

découragement (voir I.C. ci-dessus), qui est volontiers attisé par des influences étrangères, comme détaillé au I.B.4. ci-dessus. Or, **plus que jamais, il est important pour la stabilité de la région d'y entretenir un tropisme européen et atlantiste**.

En juillet 2023, le rapport d'information sénatorial précité invitait la France et l'Union européenne à « *consolider l'intégration européenne des Balkans occidentaux en diversifiant et en intensifiant leur présence dans cette région* ». A cet égard, le C3BO est porteur d'un signal d'autant plus fort qu'il permet également, en améliorant le niveau de résilience cyber des Balkans occidentaux, de les rapprocher des standards de l'Union européenne et notamment de la directive NIS2.

Le troisième enjeu pour la France est un **enjeu de *soft power*** : forte de ses compétences qui lui permettent de se positionner à l'échelle internationale comme une **puissance cyber de premier rang, responsable, coopérative et solidaire,** la France tire de son rôle cyber-diplomatique un bénéfice réputationnel important, en Europe comme en Afrique. Avec un rayonnement régional qui ne manquera pas de rejaillir sur la France, le C3BO, vitrine du savoir-faire français, viendra assurément consolider cette image.

3. **Autres bénéfices escomptés**

Du point de vue sociétal, la création du centre intègre une stratégie volontariste de renforcement de l'égalité femmes-hommes, en prévoyant notamment :

- La participation accrue des femmes aux formations délivrées par 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 communication 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. Dans un cadre plus global, le renforcement des capacités cyber permettra d'améliorer la réponse judiciaire à l'exploitation et aux abus sexuels des femmes et des enfants en ligne.

4. L'enjeu du statut d'organisation internationale

Il est cependant précisé que **l'objet de cet accord n'est pas d'autoriser la création du C3BO, qui d'ores et déjà existe et fonctionne sans nécessiter**

aucune validation par le Parlement, mais sa transformation en organisation internationale.

Ce statut devrait permettre de renforcer la sécurité juridique du centre en lui conférant une personnalité juridique internationale, dotée d'un conseil d'administration, d'une gouvernance et d'un financement dédiés. La France, la Slovénie et le Monténégro en seraient les membres fondateurs ; les 5 autres pays des Balkans occidentaux ont vocation à en devenir membres ; l'accord prévoit en outre qu'ils pourraient être rejoints le cas échéant par d'autres pays européens. La future organisation internationale présentera notamment l'avantage, par rapport au format actuel, de permettre un financement par ces futurs autres membres et, à terme, par l'Union européenne.

D. LE CONTENU DE L'ACCORD : LA MONTÉE EN PUISSANCE PROGRAMMÉE DES CAPACITÉS CYBER DE LA RÉGION

Après un préambule insistant sur la nécessité de renforcer la sécurité du cyberespace « *dans le monde entier* », **le premier article** est consacré aux définitions des termes utilisés dans l'accord, et notamment :

- celle des « *membres fondateurs* », soit la France, le Monténégro et la Slovénie,
- celle des « *autres membres appartenant au groupe des six pays des Balkans occidentaux* », soit l'Albanie, la Bosnie-Herzégovine, le Kosovo, la Macédoine du Nord et la Serbie,
- celle des « *autres membres* », soit tout pays ou organisation internationale ou régionale n'appartenant à aucune des deux précédentes catégories.

L'article 2 confère au Centre le statut juridique d'organisation internationale ; son siège est établi par **l'article 3** à Podgorica (Monténégro).

L'objectif du C3BO tel que défini par **l'article 4** est le renforcement de la cyber-résilience de la région, grâce à l'organisation de formations, au développement d'échanges d'informations et de bonnes pratiques, et à l'élaboration d'une maquette de cours universitaires sur les questions cyber.

La deuxième partie (**articles 5 à 8**) définit les qualités des différentes catégories de membres ainsi que leurs modalités de participation au conseil d'administration ; chacun d'eux devra notamment s'acquitter d'une contribution annuelle dont le montant est fixé par le conseil d'administration.

Les principaux organes du C3BO sont décrits en troisième partie de l'accord :

- le conseil d'administration, au sein duquel chaque membre fondateur dispose de deux représentants et chaque autre membre d'un représentant, qui supervise les activités du Centre selon les modalités précisées **à l'article 10** ;

- le conseil consultatif (décrit **à l'article 11**), au sein duquel chaque membre dispose d'un représentant, qui élabore et propose au conseil d'administration le programme de travail ainsi qu'un plan pluriannuel de développement ;
- le secrétariat, dont le directeur général, représentant légal du C3BO, est désigné par le conseil d'administration (**article 12**).

En vertu de **l'article 13**, le financement du Centre est assuré par les contributions financières et en nature des différents membres, dont les montants respectifs sont fixés par le conseil d'administration, ainsi que, le cas échéant, par des participations apportées par des partenaires ou des bailleurs de fonds.

L'article 14 stipule que le règlement intérieur du Centre est voté par le conseil d'administration, à la majorité des deux tiers. Ce règlement intérieur définit notamment les règles relatives à la protection des données (**article 15**).

Conformément à **l'article 16**, tout personnel recruté par le Centre devra être soumis à une procédure d'habilitation conforme au droit interne des membres fondateurs.

La partie VII (**articles 17 à 24**) est consacrée aux dispositions finales classiques, soit les modalités de réserve, signature, ratification, approbation, adhésion, entrée en vigueur, amendement, retrait, dénonciation et règlement des différends ; le Monténégro est désigné comme dépositaire de l'accord.

*

* *

L'accord faisant l'objet du présent rapport est un projet-phare qui contribuera à développer la cyber-résilience des pays des Balkans occidentaux, et, par là-même, celle de leurs partenaires européens et français. Il contribue également à mettre en avant la compétence de la France comme puissance cyber de premier rang, responsable, coopérative et solidaire, dans une zone d'importance géostratégique majeure, où l'influence européenne et atlantiste est mise à mal par des ingérences malveillantes.

Il fait l'objet de la part de la commission de deux recommandations :

- la première est de tendre, pour l'avenir et au fur et à mesure que l'organisation internationale s'enrichira de nouveaux membres, vers une répartition moins déséquilibrée des contributions financières entre les membres ;

- la seconde est que les formations soient conditionnées à une participation financière, au moins symbolique, des bénéficiaires.

EXAMEN EN COMMISSION

Réunie le mercredi 29 janvier 2025, sous la présidence de M. Cédric Perrin, président, la commission des affaires étrangères, de la défense et des forces armées a procédé à l'examen du rapport de Mme Sylvie Goy-Chavent sur le projet de loi n° 166 (2024-2025) autorisant l'approbation de l'accord portant création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO).

Mme Sylvie Goy-Chavent, rapporteur. – Le projet de loi qui vous est soumis aujourd'hui a pour objet l'accord, signé à Tirana le 16 octobre 2023 entre la France, le Monténégro et la République de Slovénie, relatif à la création du Centre de développement des capacités cyber dans les Balkans occidentaux (C3BO). Je le rappelle, les pays des Balkans occidentaux sont : le Monténégro, l'Albanie, la Serbie, la Macédoine du Nord, la Bosnie-Herzégovine, le Kosovo.

Le concept de cyberespace, apparu dans les romans de science-fiction des années 1980, est aujourd'hui entré dans notre quotidien et, avec lui, la menace des multiples « scénarios catastrophe » auxquels il est exposé.

Pour dépeindre les différents types d'attaquants, on parle d'ordinaire de « hackers à chapeau noir, gris ou blanc », selon que leurs intentions sont plus ou moins malveillantes. Ce monde hétérogène est principalement constitué de trois catégories d'agresseurs : tout d'abord les agresseurs étatiques ou assimilés, particulièrement chevronnés et offensifs, conduisant une guerre hybride qui n'épargne pas la France ; ensuite des cybercriminels, qui ciblent désormais l'ensemble du tissu social – PME, établissements de santé, particuliers… – ; et, enfin, les « hacktivistes », qui conduisent, pour des raisons militantes, des attaques cyber qu'ils jugent légitimes à défaut d'être légales.

La montée en puissance de cette menace est devenue une préoccupation majeure, notamment pour les démocraties, particulièrement visées. À l'échelle mondiale, le coût des attaques cybercriminelles est estimé aujourd'hui à 9 220 milliards de dollars et pourrait atteindre en 2029 15 630 milliards de dollars, un peu plus que le PIB de la Chine…

Cette intensification de la menace s'explique par plusieurs évolutions particulièrement alarmantes.

D'abord, sur le *dark web*, sont mis à disposition des cybercriminels des kits d'agression clefs en main, grâce auxquels lancer un rançongiciel de manière automatisée et récupérer en bitcoins la rançon extorquée est devenu à la portée d'un internaute de niveau moyen.

Par ailleurs, des prestataires spécialisés se sont développés, proposant à leurs clients, le plus souvent étatiques, des outils de piratage élaborés, des

analyses ciblées des vulnérabilités ou bien des offres d'expertise personnalisées.

L'intelligence artificielle, qui permet de concevoir ou de contrefaire un site, un courriel, une photo ou encore une voix, mais aussi de mieux cibler les victimes, s'est également mise au service des cybercriminels pour élaborer des attaques de plus en plus sophistiquées.

Enfin, je souhaite insister sur le fait que nous sommes maintenant confrontés à un milieu de mieux en mieux structuré, qui constitue un véritable écosystème de la cybercriminalité, avec des forums permettant l'échange de données, l'achat de logiciels malveillants, mais aussi des liens vers des prestataires de cyberattaque ou des circuits de blanchiment…

Face à ces menaces, les parades possibles reposent pour l'essentiel sur les politiques de prévention et de formation, afin de sensibiliser un public le plus large possible aux bonnes pratiques de sécurisation.

C'est dans cet objectif qu'a été créé, en novembre 2022, le C3BO, implanté à Podgorica, au Monténégro. Sur le modèle des écoles nationales à vocation régionale, implantées essentiellement en Afrique, le Centre délivre des formations à la cybersécurité et à la lutte contre la cybercriminalité, et favorise le partage des bonnes pratiques.

Son budget annuel s'élève à 1,05 million d'euros, essentiellement supporté par la partie française, avec une participation de 870 000 euros, soit 83 % du budget total – j'y reviendrai –, contre 100 000 euros pour la Slovénie et 80 000 euros pour le Monténégro.

Le Centre dispense, à titre gratuit – j'y reviendrai également –, des formations thématiques d'une semaine, au bénéfice tant des services de police et des magistrats que des administrations et des militaires. Il a délivré, en 2023, année de sa mise en service, 5 formations ; en 2024, il est monté en puissance, avec 21 formations, destinées à 400 stagiaires ; en 2025, il atteindra sa vitesse de croisière avec 31 formations, soit près de huit mois de cours, qui bénéficieront à quelque 600 stagiaires. Il propose également un cursus universitaire de haut niveau et diplômant.

Pour la diplomatie française, l'enjeu du C3BO est triple.

Tout d'abord, bien sûr, il présente un enjeu de cybersécurité. Du fait de leur insuffisante culture de cybersécurité, les pays des Balkans occidentaux sont particulièrement vulnérables : on l'a vu avec l'offensive perpétrée par la Russie contre le Monténégro, en 2022, en raison de sa position dans le conflit ukrainien, et avec celle qui a été lancée par l'Iran à l'encontre de l'Albanie, la même année, en représailles à l'hospitalité accordée aux moudjahidin du peuple. Or relève de l'intérêt général, y compris de celui de la France, de renforcer la cyber-résilience de nos partenaires, afin d'éviter toute compromission, par rebond, de notre propre cyberespace. Cette même problématique se pose avec une acuité particulière dans le cadre de

l'Organisation du traité de l'Atlantique Nord (Otan), et explique que, en même temps que la France et la Slovénie, les États-Unis se préoccupent de la cybersécurité des Balkans occidentaux au point d'installer également au Monténégro un centre cyber, doté de missions complémentaires à celles du C3BO.

En second lieu, la région des Balkans occidentaux constitue un enjeu géostratégique majeur : dans un contexte où le processus d'adhésion à l'Union européenne de ces pays est particulièrement lent, voire en panne, leur enthousiasme proeuropéen a tendance à s'émousser et ouvre la brèche à un réel découragement, volontiers attisé par des influences étrangères. Or, plus que jamais, il est important pour la stabilité de la région d'y entretenir un tropisme européen et atlantiste. En juillet 2023, l'excellent rapport d'information de nos collègues Cigolotti, Conway-Mouret, Fournier et Gréaume invitait la France et l'Union européenne à « consolider l'intégration européenne des Balkans occidentaux en diversifiant et en intensifiant leur présence dans cette région ». À cet égard, le C3BO est porteur d'un signal d'autant plus fort qu'il permet également, en améliorant le niveau de cyber-résilience des Balkans occidentaux, de les rapprocher des standards de l'Union européenne, notamment de la directive NIS 2 (*Network and Information Security*).

Le troisième enjeu pour la France est un enjeu de *soft power* : forte de ses compétences, qui lui permettent de se positionner à l'échelle internationale comme une puissance cyber de premier rang, responsable, coopérative et solidaire, la France tire de son rôle cyberdiplomatique un bénéfice réputationnel important, en Europe comme en Afrique. Avec un rayonnement régional, qui ne manquera pas de rejaillir sur la France, le C3BO viendra assurément consolider cette image.

Je précise que l'objet de cet accord est d'autoriser non pas la création du C3BO, ce qui ne nécessiterait aucune validation par le Parlement, mais sa transformation en organisation internationale. Ce statut devrait permettre de renforcer la sécurité juridique du Centre en lui conférant une personnalité juridique internationale, dotée d'un conseil d'administration, d'une gouvernance et d'un financement spécifiques. La France, la Slovénie et le Monténégro en seraient les membres fondateurs ; les cinq autres pays des Balkans occidentaux ont vocation à en devenir membres et l'accord prévoit en outre qu'ils pourraient être rejoints, le cas échéant, par d'autres pays européens. La future organisation internationale présentera notamment l'avantage, par rapport au format actuel, de permettre un financement par les futurs autres membres et, à terme, par l'Union européenne.

Mes chers collègues, je vous proposerai d'approuver ce texte, qui, en même temps qu'il favorise la montée en puissance d'un établissement phare consacré à la cybersécurité, renforcera la présence française dans une région stratégique.

Cependant, je vous propose d'assortir votre accord de deux recommandations, toutes deux relatives au financement du centre :

- la première, dans le contexte budgétaire dans lequel nous nous trouvons, serait de tendre, pour l'avenir et au fur et à mesure que l'organisation internationale s'enrichira de nouveaux membres, vers une répartition moins déséquilibrée des contributions financières entre les membres ;

- la seconde, dans le même sens, serait que les formations, qui à l'heure actuelle sont dispensées de façon entièrement gratuite, ce qui inclut les frais de transport, d'hébergement et de séjour, soient conditionnées à une participation financière, au moins symbolique, des bénéficiaires.

Ces deux recommandations, sans remettre en cause ni l'ambition du projet ni le rôle pilote joué par la France, me semblent de nature à alléger et à mieux répartir le coût de ce centre. Si vous en êtes d'accord, je les communiquerai au Quai d'Orsay.

Ce texte est également pour moi l'occasion d'émettre ici une suggestion : nous devrions engager une réflexion sur la manière dont notre commission pourrait assurer le suivi de tels organismes, par exemple dans le cadre de l'avis budgétaire sur le programme 105, ou par le biais d'auditions ou de rapports d'activité.

Je vous précise enfin que l'examen en séance publique de cette convention pourrait se tenir au cours de la première quinzaine de février, selon une procédure simplifiée, ce à quoi la Conférence des présidents, de même que votre rapporteur, a souscrit.

Mme Michelle Gréaume. – Vous avez abordé la question de la prise en charge du financement par chaque État membre. Combien cela coûtera-t-il à chacun ?

Mme Sylvie Goy-Chavent, rapporteur. – À l'heure actuelle, la France prend en charge 870 000 euros, la Slovénie 100 000 euros et le Monténégro, qui fournit les locaux, 80 000 euros. L'idée de l'érection du Centre en organisation internationale serait d'élargir ce financement à d'autres membres.

M. Olivier Cadic. – La création de ce centre fait suite à l'attaque subie par le Monténégro à l'été 2022, touchant 17 systèmes et 3 000 ordinateurs dans 10 ministères. L'Agence nationale de la sécurité des systèmes d'information (Anssi) avait été dépêchée sur place pour les aider, dans le cadre de sa première intervention internationale. Il faut se rendre compte de ce qu'est le Monténégro, c'est l'équivalent d'un département français comme la Gironde. Ce pays ne peut pas faire face seul à de telles attaques, surtout que l'attaque émanait de la Russie, qui entendait ainsi punir ce pays parce qu'il rejoignait l'Otan. L'Anssi a donc ainsi pu travailler pour la première fois à l'international et la France a pu aider ces pays à élever leur niveau en la matière.

Combien ces cours représentent-ils en temps homme ? Qui délivre ces formations ? Est-ce l'Anssi ? Est-ce pris sur son budget ? Dans ce cas, nous pourrions le contrôler au travers du programme 129.

Mme Sylvie Goy-Chavent, rapporteur. – Pas du tout, les formateurs appartiennent à la gendarmerie ou sont des formateurs privés. Le budget de l'Anssi n'est pas affecté. Ces crédits relèvent du programme 105.

M. Mickaël Vallet. – La France est à l'initiative de cette organisation internationale et la finance largement. Quelle en sera la langue de travail ? Dans quelles langues les cours sont-ils dispensés ? Je n'ai aucun problème à ce qu'ils ne soient pas donnés en français, mais est-ce donné dans la langue des stagiaires ?

Mme Sylvie Goy-Chavent, rapporteur. – Les cours sont donnés pour l'essentiel en anglais.

M. Mickaël Vallet. – Je glisserais bien une recommandation sur le sujet, en distinguant entre la langue de travail et la langue des cours, afin de favoriser la langue française.

Mme Sylvie Goy-Chavent, rapporteur. – Le niveau des stagiaires est très élevé. Ils parlent tous l'anglais, la langue véhiculaire.

M. Mickaël Vallet. – Mais quelle sera la langue de travail de l'organisation ?

Mme Sylvie Goy-Chavent, rapporteur. – Il y a trois personnes qui s'occupent de la gestion de l'organisation. Je poserai la question pour savoir en quelle langue ils travaillent.

Le projet de loi est adopté sans modification.

ANNEXE 1 : LISTE DES PERSONNES AUDITIONNÉES

Pour le Ministère de l'Europe et des affaires étrangères :

- Mme Reachbha FITZGERALD, FITZGERALD, chargée de mission C3BO, Sous-direction de l'Europe balkanique ;

- M. Guillaume NARJOLLET, Adjoint au Sous-Directeur, Sous-direction des questions multilatérales et sectorielles, Direction de la coopération de sécurité et de défense ;

- M. Lieutenant-Colonel Gilles SCHWOERER, Officier référent Cyber à la Sous-direction des questions multilatérales et sectorielles, Direction de la coopération de sécurité et de défense ;

- Mme Gabrielle MISERE, Sous-directrice adjointe de la Cybersécurité, Direction des affaires stratégiques, de sécurité et du désarmement ;

- M. Mahé DERSOIR, Rédacteur, Sous-direction de la Cybersécurité, Direction des affaires stratégiques, de sécurité et du désarmement ;

- Mme COSTA DE BEAUREGARD, Sous-Directrice de l'Europe balkanique, Direction de l'Europe continentale ;

- M. Pierre DOUSSET, conseiller juridique à la Mission des Accords et Traités, Direction des affaires juridiques.