



EUROPEAN
UNION AGENCY
FOR CYBERSECURITY

L'AGENCE DE L'UNION EUROPÉENNE POUR LA CYBERSÉCURITÉ

UNE AGENCE PROPICE AU PHÉNOMÈNE DE MOBILITÉ PRIVÉ-PUBLIC ?

M2 APE
Cassandre GUÉNON
Julia CLAMADIEU
Angèle LOISEAU



Table des matières

I/ INTRODUCTION.....	2
a) Présentation de l'Agence	2
b) Transparence, Gouvernance et Gestion des conflits d'intérêts au sein de l'ENISA....	2
II/ MÉTHODOLOGIE	3
a) Enjeux de la recherche.....	3
b) Composition de l'échantillon	4
c) Méthodes et procédés d'analyse	5
d) Limites et difficultés rencontrées.....	6
III/ INTERPRÉTATION DES RÉSULTATS	6
a) L'indicateur de sexe.....	6
b) Répartition des nationalités au sein de l'agence	8
c) Type de diplôme obtenu et phénomène d'eurocéanisation des études	9
d) Domaine d'études des acteurs.....	9
e) Carrières et secteur d'expérience professionnelle.....	11
f) Mobilités privé-public	18
IV/ CONCLUSION	19
Annexes.....	21
Organigramme actuel (décembre 2024).....	21
Ancien organigramme	21
Liste des entreprises dans lesquelles les individus ont travaillé	22
Exemple d'une déclaration d'intérêts : celle de Juhani Lepassaar, Directeur exécutif....	22

I/ INTRODUCTION

a) Présentation de l'Agence

Depuis les années 80, on observe au sein de l'UE un transfert progressif de compétences des bureaucraties centrales vers des agences spécialisées, destinées à fournir une expertise stratégique et à renforcer la coopération entre États membres. L'Agence européenne pour la cybersécurité (ENISA) incarne cette dynamique face aux risques numériques croissants. Créée en 2004 (règlement CE n° 460/2004), l'ENISA est basée à Héraklion (Crète) et dispose d'un bureau à Athènes. Née dans un contexte de montée des cybermenaces et de dépendance aux TIC, elle a pour mission de coordonner les efforts européens pour sécuriser les infrastructures numériques. Son rôle, initialement centré sur la coopération entre États membres, a été élargi par le Cybersecurity Act (2019), qui lui a attribué de nouvelles responsabilités, telles que la certification des produits et services numériques.

L'ENISA est devenue un acteur clé de la cybersécurité européenne, avec des missions variées : appui aux stratégies nationales, gestion de crises cybernétiques, organisation d'exercices comme « Cyber Europe », et développement de schémas de certification pour assurer la sécurité des produits numériques. Elle mène également des initiatives de sensibilisation, de formation, et publie des rapports prospectifs sur les cybermenaces émergentes. Le positionnement de l'ENISA soulève des interrogations sur l'indépendance de son expertise. Le phénomène des « portes tournantes » (revolving door), marqué par le passage de ses membres entre des postes dans l'industrie régulée et des fonctions réglementaires, met en lumière les interactions entre régulateurs publics et acteurs privés. L'étude de ces dynamiques internes permettrait d'évaluer l'impact de ces relations sur la production de régulations et la gestion des cybermenaces, s'inscrivant dans les débats sur la gouvernance des agences spécialisées et leur capacité à conjuguer efficacité et neutralité.

b) Transparence, Gouvernance et Gestion des conflits d'intérêts au sein de l'ENISA

L'ENISA applique des règles de gouvernance pour garantir la transparence et prévenir les conflits d'intérêts, en s'appuyant sur les articles 25 à 28 du Cybersecurity Act. L'agence affirme “*s'efforcer de conduire son travail aussi ouvertement que possible et de s'assurer qu'elle mène ses activités avec un haut niveau de transparence.*” Pour se faire, elle publie diverses informations sur son site, notamment les calendriers des réunions de direction, les marchés publics et certains documents stratégiques. Pour les documents non accessibles, elle applique les principes de transparence du Traité de Lisbonne, permettant aux citoyens européens d'en demander l'accès. L'ENISA a également adopté un Code de bonne conduite s'appliquant à son personnel et aux personnes en interaction avec elle.

En matière de conflits d'intérêts, l'article 25 du Cybersecurity Act impose aux membres du conseil d'administration, au directeur exécutif et aux experts externes de remplir des déclarations d'intérêts annuelles, et de signaler tout conflit potentiel en début de réunion. L'article 26 renforce cette transparence en exigeant leur publication. Bien que l'agence soit peu exposée dans le débat public et n'ait pas fait l'objet de scandales liés à d'éventuels conflits d'intérêts, certains éléments soulèvent néanmoins des interrogations à ce sujet. Certaines déclarations d'intérêts restent inaccessibles : celles des membres du Management Board ne sont pas toutes accessibles, et celles de l'Advisory Group sont soumises à des restrictions d'accès. Par ailleurs, aucune obligation similaire ne s'applique aux autres agents occupant des postes à responsabilité. Aussi, contrairement à certaines agences comme l'EFSA, l'ENISA ne prévoit pas de période de cooling-off, ni de mesures spécifiques contre la capture réglementaire. Ajoutons à cela que le site de l'ENISA mentionne une page dédiée aux "*Règles pour la prévention et la gestion des conflits d'intérêts*". Son accès est restreint. Une telle limitation est regrettable, car ces informations auraient pu offrir un éclairage précieux pour approfondir cette analyse.

Concernant la gouvernance, le Management Board est composé de membres désignés par les États membres, qui élisent ensuite la présidence et le Conseil exécutif. L'ENISA publie ses offres d'emploi avec des critères de sélection spécifiques pour chaque poste. L'agence défend le principe d'égalité des chances, garantissant une sélection sans discrimination liée à la nationalité, au genre, à l'âge ou aux convictions personnelles. Elle recrute non seulement des experts en cybersécurité, mais également des professionnels dans divers domaines tels que l'administration, la communication, les ressources humaines, etc. Il n'existe donc pas de profil unique recherché. Les candidats doivent toutefois être ressortissants de l'UE, et leurs diplômes obtenus hors de l'Union doivent être reconnus par un État membre. De plus, toute interaction entre un candidat et les agents impliqués dans son recrutement est interdite afin d'assurer l'impartialité du processus.

III/ MÉTHODOLOGIE

a) Enjeux de la recherche

Notre étude s'intéresse à la pratique des "revolving door", qui renvoie à des "mouvements de va-et-vient entre les secteurs privé et public"¹, au sein de l'agence ENISA, une agence relativement discrète. En s'appuyant sur une analyse approfondie des trajectoires professionnelles et des caractéristiques sociales d'un groupe restreint d'individus, cette étude met en évidence des tendances communes. Ces résultats sont ensuite comparés aux dynamiques observées dans d'autres agences étudiées,

¹ Raymond Hudon, Stéphanie Yates et Mathieu Ouimet, "Portes tournantes et éthique démocratique", *Éthique publique*, vol. 18, n° 2, 2016

permettant ainsi de dégager des similitudes et des spécificités propres à chaque contexte.

La troisième partie de la recherche se concentre sur des aspects tels que le sexe, le niveau et le domaine de formation, l'expérience dans le secteur privé ou encore l'âge des individus concernés. L'objectif est de déterminer si ce phénomène des "revolving door" est significatif au sein de l'agence et, le cas échéant, d'en dégager un profil représentatif. Enfin, l'étude cherche à décrypter les dynamiques internes et à identifier les rôles susceptibles d'influencer ce mécanisme. Elle vise ainsi à mieux comprendre les interactions entre les parcours individuels et les processus décisionnels de l'agence.

b) Composition de l'échantillon

La composition de notre échantillon a constitué la première étape de notre travail. Nous nous sommes d'abord intéressées à la structure de l'agence, qui se divise en cinq organes officiels : un Management Board, un Executive Board et un Directeur exécutif, un National Liaison Officers Network (NLO Network) et un Advisory Group. Ce modèle organisationnel est assez commun à toutes les agences, bien qu'elles traitent de domaines différents et spécialisés.

Pour poursuivre notre sélection, nous nous sommes basées sur deux éléments principaux : la permanence des membres au sein de l'ENISA et le rôle qu'ils y occupent. Nous avons choisi de concentrer notre échantillon sur des personnes permanentes, plutôt qu'intermittentes², occupant des postes à responsabilité ou des fonctions clés au sein de l'agence. L'objectif est d'identifier les principaux régulateurs ayant un impact direct sur les activités essentielles assignées à l'agence.

Sur cette base, nous avons exclu plusieurs catégories de membres. D'abord, le Groupe Consultatif, bien qu'il rassemble des experts de divers horizons (industrie, monde académique, entreprises, organisations de consommateurs) et qu'il joue un rôle important, il reste purement consultatif. Ses membres ne sont ni permanents, ni décisionnaires, ni impliqués directement dans les fonctions de régulation. Pour des raisons similaires, nous avons aussi écarté les membres du NLO Network, composé de représentants des États membres assurant la liaison avec l'agence, et les membres de Management Board (à l'exception de la présidence) réunissant des représentants des États membres, d'États tiers et de la Commission. Encore une fois, ces membres ne sont pas des permanents et ne contribuent pas directement aux activités essentielles de l'ENISA.

Dans un premier temps, notre échantillon a alors été constitué des cadres dirigeants actuels quiassument les plus grandes responsabilités dans l'exécution des missions directes de l'agence. Cela inclut les Présidents et Vice-Présidents du Management Board et de l'Executive Board, le Directeur exécutif, ainsi que les Chefs

² Didier Georgakakis, Le champs de l'Eurocratie, 2012.

d'unité, de secteur et d'équipe, à l'exclusion de ceux exerçant des fonctions purement administratives ou liées aux ressources humaines. Pour obtenir un échantillon plus large, permettant des données plus représentatives et comparables à celles d'autres agences, nous avons également inclus selon les mêmes critères neuf personnes de l'organigramme précédent (2020) qui occupaient des postes équivalents.

L'échantillon se compose désormais de 29 personnes sur environ une centaine d'agents travaillant à l'ENISA³.

c) **Méthodes et procédés d'analyse**

Nous avons choisi de fonder notre travail sur une méthode d'analyse quantitative spécifique : la prosopographie. Largement utilisée dans les sciences sociales, cette approche permet de mettre en lumière des caractéristiques distinctives des profils des individus constituant le groupe étudié. Cette méthode est d'autant plus pertinente dans le cadre d'une enquête collective comme celle-ci, où le travail des différents groupes a permis d'enrichir la base de données communes ainsi que la comparaison des résultats entre les agences. Une fois les 29 acteurs pertinents identifiés, composant notre échantillon, nous avons entamé la collecte des données personnelles relatives à leurs profils et parcours. Cette étape s'est avérée complexe, notamment en raison de la quantité limitée de données officielles publiées par l'ENISA. Par conséquent, la grande majorité des données est issue des profils LinkedIn des individus, et dans une moindre mesure, de leurs pages Wikipédia ou d'autres sites internet, lorsque disponibles. Par ailleurs, un autre outil clé dans notre recherche a été la plateforme Internet Archive, qui nous a permis de remonter dans le temps pour accéder aux noms des anciens occupants des postes qui nous intéressaient. Pour certains postes de haut niveau, tels que le Directeur exécutif et certains anciens Présidents et Vice-Présidents du Management Board, cela nous a aussi permis de retrouver leurs anciennes déclarations d'intérêts, autrefois disponibles sur le site de l'ENISA.

La collecte des données a permis, pour chaque acteur, de renseigner un large éventail d'informations personnelles via un formulaire de saisie. Ces informations incluent la nationalité, l'âge, le niveau d'études, le premier emploi, ou encore la proportion de temps de travail consacrée au secteur privé. À partir de ces données, un tableur Excel a été créé pour rassembler l'ensemble des informations collectées par les différents groupes ayant travaillé sur d'autres agences européennes, aussi bien cette année que l'année précédente. Ce tableau a également permis de comparer les données entre les différentes agences, facilitant ainsi une analyse croisée des résultats. Par ailleurs, Excel a joué un rôle central dans ce projet, servant à la fois d'outil pour effectuer les analyses statistiques et pour produire les tableaux et graphiques présentés dans ce rapport.

³ Voir les organigrammes en annexes.

d) Limites et difficultés rencontrées

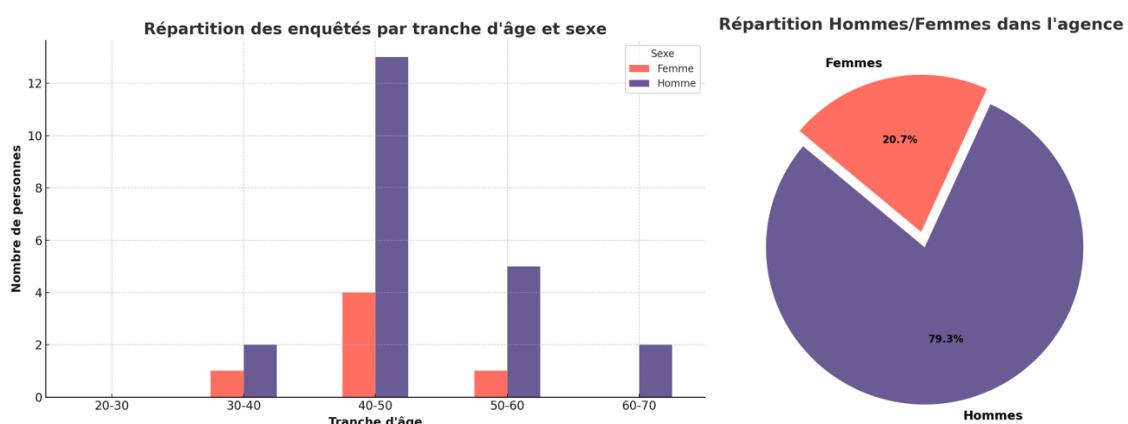
Cette recherche présente des limites méthodologiques qui méritent d'être soulignées. Le recours à un échantillon de 29 individus empêche de représenter pleinement les dynamiques internes et les rapports de force spécifiques à l'ENISA. Vu la complexité du champ eurocratique, l'enquête n'a pas pour ambition d'offrir une évaluation exhaustive du phénomène des portes tournantes. Les postes analysés ont été sélectionnés après réflexion, et ceux écartés l'ont été pour leur faible pertinence.

Des difficultés pratiques ont freiné la collecte de données, notamment le manque de données officielles publiées par l'ENISA. Bien que les règles de transparence prévoient une déclaration d'intérêt pour chaque membre, seules celles des principaux dirigeants et des représentants des États sont accessibles. L'administration a confirmé qu'elle ne pouvait divulguer les déclarations des autres membres pour raisons de confidentialité.

L'utilisation de LinkedIn pose également des limites d'objectivité. Cette plateforme reflète souvent une construction narrative personnelle et les profils sont parfois incomplets ou obsolètes. Certaines informations comme l'âge ou la nationalité ont dû être estimées. Enfin, le recours à Internet Archives pour identifier d'anciens collaborateurs a été difficile en raison des changements dans les dénominations de postes, la structure interne de l'ENISA, et la variabilité des données publiées au fil des années.

III/ INTERPRÉTATION DES RÉSULTATS

a) L'indicateur de sexe



Le graphique révèle que notre échantillon est composé de près de 80 % d'hommes (23 hommes). Cette sur-représentation masculine est cohérente avec les tendances globales dans les domaines technologiques et scientifiques, où les hommes occupent historiquement la majorité des postes. En effet, l'étude par tranches d'âge

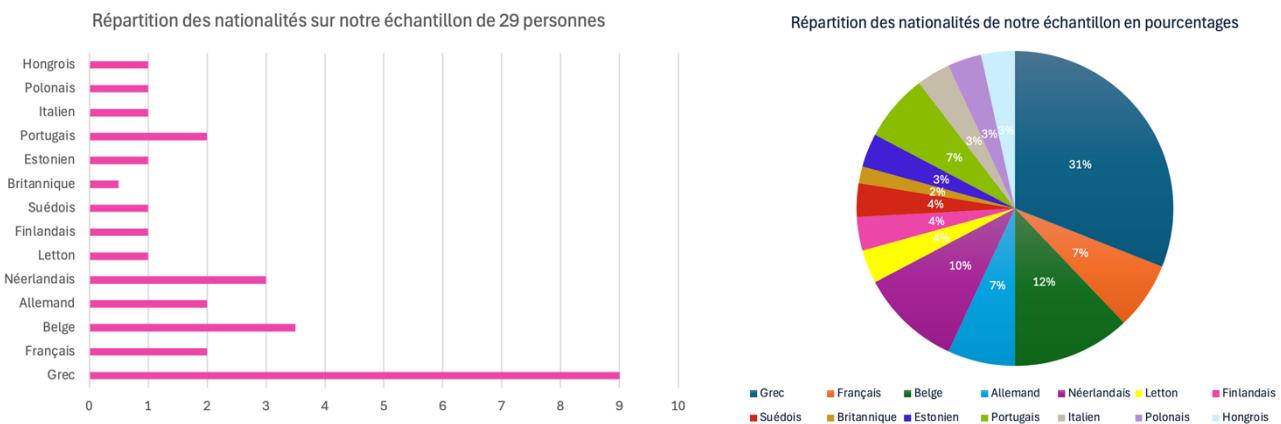
montre une concentration particulièrement élevée d'hommes dans la catégorie 40-50 ans, où ils représentent une grande majorité des enquêtés, avec 12 personnes masculines dans cette tranche. Cela peut refléter une exigence d'expérience dans le domaine, où les compétences techniques spécialisées sont souvent acquises après plusieurs années de carrière. Les femmes représentent seulement 20,7 % de nos enquêtés et dans certaines tranches d'âge, leur présence est marginale, voire inexiste. En effet, la faible proportion féminine dans les tranches 40-50 ans et 50-60 ans témoigne d'un accès limité pour les femmes aux postes de leadership à l'ENISA.

Selon des rapports tels que celui d'International Information System Security Certification Consortium, les femmes représentent environ 24 % de la main-d'œuvre en cybersécurité mondiale, ce qui reste faible en comparaison d'autres secteurs. Historiquement, les filières STEM (Science, Technologie, Ingénierie, Mathématiques), qui forment la base des compétences en cybersécurité, attirent moins de femmes. En Europe, en 2021, seulement 19 % des diplômés en ingénierie informatique étaient des femmes (Eurostat). Cela peut s'expliquer par le fait que la cybersécurité est souvent associée à des compétences techniques avancées (ex. cryptographie, sécurité des réseaux), perçues comme des domaines masculins.

L'ENISA se situe dans la moyenne des agences en termes de répartition hommes-femmes, avec une proportion d'environ 80 % d'hommes et 20 % de femmes. Certaines agences, comme Eurofound ou EUIPO, présentent une répartition plus équilibrée, voire inversée, avec une majorité féminine. À l'opposé, des agences comme l'EMA affichent également une forte prédominance masculine, similaire à l'ENISA. Cette comparaison souligne que la sous-représentation féminine reste un défi récurrent, particulièrement dans les agences liées à la technologie ou aux sciences, reflétant des tendances structurelles communes dans ces domaines.

Dans ce contexte, il est pertinent de s'intéresser à la représentation féminine au sein de la DG CONNECT de la Commission européenne. À sa tête, une femme occupe le poste de commissaire, et la cheffe d'unité "cyber" ainsi que la conseillère principale sont également des femmes. De plus, deux des trois directeurs généraux adjoints sont des femmes, ce qui souligne la reconnaissance des compétences féminines dans les fonctions stratégiques. En élargissant l'analyse à l'ensemble du personnel de la DG CONNECT (hors commissaire), on dénombre 31 femmes contre 36 hommes, soit une proportion féminine d'environ 46,3 %. Cela montre un léger déséquilibre en défaveur des femmes, mais témoigne également d'une tendance vers une meilleure inclusion. Comparée à l'ENISA, la DG CONNECT affiche une représentation féminine relativement plus équilibrée dans un domaine technologique traditionnellement dominé par les hommes, bien que 6 des 10 chefs d'unité restent des hommes.

b) Répartition des nationalités au sein de l'agence



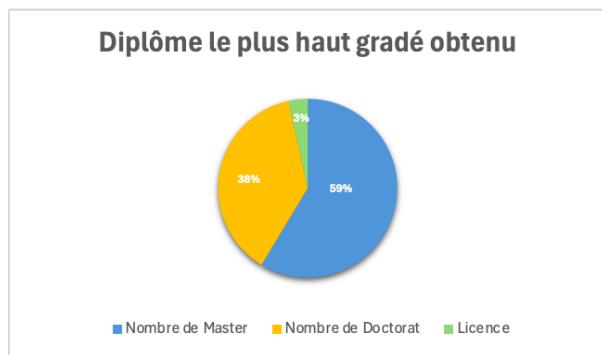
Notre échantillon met en évidence une diversité nationale au sein de l'ENISA, avec 13 États membres représentés. Comme à l'Agence européenne pour l'environnement, cette pluralité reflète l'inclusivité et la représentativité des pays de l'UE dans le domaine de la cybersécurité.

On observe une forte présence de membres d'origine grecque, représentant près d'un tiers de l'effectif. Cette tendance est liée à l'implantation des bureaux de l'ENISA à Athènes et Héraklion. Ce phénomène se retrouve dans d'autres agences de l'UE, comme l'Agence européenne de contrôle des pêches, l'Office de l'UE pour la propriété intellectuelle ou l'Agence de coopération des régulateurs de l'énergie, où la nationalité dominante correspond souvent au pays d'accueil. Toutefois, cette tendance n'est pas systématique, comme le montre l'exemple de l'Autorité européenne de sécurité des aliments.

Les pays nordiques (Lettonie, Estonie, Suède, Finlande) sont bien représentés, totalisant 4 membres sur 29. Leur engagement en cybersécurité repose sur une expertise technologique reconnue et, pour certains, sur leur proximité avec la Russie, qui renforce leur besoin de protection numérique. Le personnel belge et néerlandais suit de près, les Pays-Bas jouant un rôle clé en tant que hub technologique européen. Selon le classement 2023 du MIT Technology Review Insight, ce pays se classe deuxième parmi les plus investis en cybersécurité au niveau mondial⁴, ce qui peut expliquer la présence notable des Néerlandais à l'ENISA. Enfin, les nationalités française, allemande et portugaise sont également bien représentées. La France et l'Allemagne, moteurs de l'UE, disposent sans doute de plus de ressources humaines dans ce domaine, mais leur implication pourrait aussi découler de leur exposition accrue aux cybermenaces.

⁴ Cyber-Management School, Les pays les plus avancés en matière de cybersécurité, Actualités, 10 juin 2024. <https://www.cyber-management-school.com/actualite/les-pays-les-plus-avances-en-matiere-de-cybersecurite/>

c) Type de diplôme obtenu et phénomène d'europeanisation des études



Parmi les 29 acteurs étudiés, 59 % (17 personnes) ont un Master comme plus haut diplôme, tandis que 38 % (11 personnes) sont titulaires d'un doctorat, soulignant un haut niveau de qualification. Les docteurs occupent généralement des postes clés, notamment dans les unités techniques (ex : Data Protection Officer, Sector Security and Infrastructure) ou à haute responsabilité (un Directeur Exécutif est docteur). Seule une personne possède une licence comme diplôme le plus élevé. Comparée aux autres agences, cette proportion de doctorants est dans la moyenne, puisque l'ensemble des agences analysées affiche un taux moyen de doctorats légèrement inférieur à 40 %.

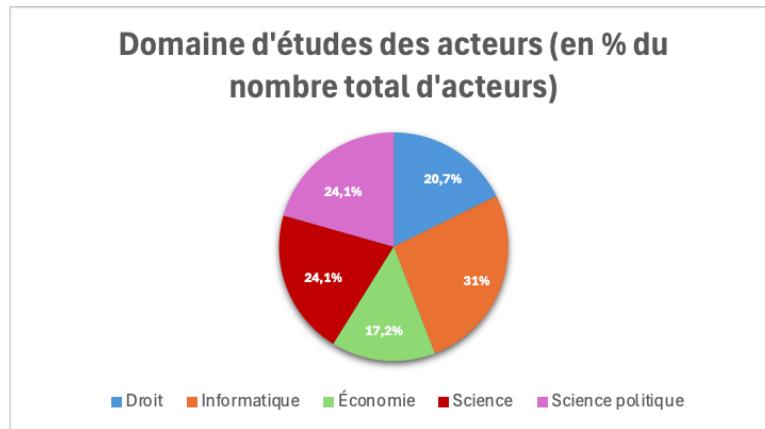
L'analyse par genre révèle que 43 % des hommes (10 sur 23) ont un doctorat contre 17 % des femmes (1 sur 6). À l'inverse, 83 % des femmes (5 sur 6) et 52 % des hommes (12 sur 23) détiennent un Master. Le seul titulaire d'une licence est un homme. Ces données montrent que les hommes sont surreprésentés au niveau doctoral, en partie en raison de la prédominance des sciences et de l'informatique, domaines historiquement masculins. Cette tendance sera approfondie dans la suite de l'analyse.

Parmi notre échantillon, 12 individus ont étudié à l'étranger, soit une proportion notable mais non majoritaire. Cela témoigne d'une certaine europeanisation des parcours académiques, sans pour autant indiquer une généralisation de la mobilité au moment des études, au sein de l'ENISA.

d) Domaine d'études des acteurs

Notre échantillon dispose-t-il d'une expertise spécifique ? Si oui, quel type d'expertise semble majoritairement reconnu par l'agence ?

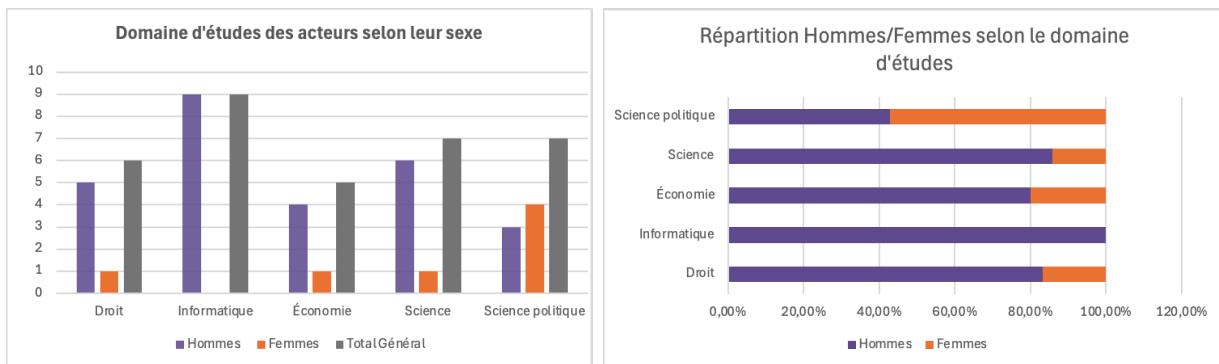
L'étude de notre échantillon révèle une diversité des parcours des acteurs de l'ENISA, regroupés en cinq domaines : droit, science politique, économie/finance, sciences et informatique. Parmi les 29 acteurs étudiés, beaucoup ont suivi plusieurs formations, parfois dans un même domaine, tandis que 5 ont un parcours pluridisciplinaire.



L'informatique est le domaine le plus représenté, avec 9 des 29 acteurs (soit 31%) ayant suivi au moins une formation dans ce domaine incluant l'ingénierie, les systèmes d'information et la cybersécurité. Si l'on ajoute les acteurs ayant une formation en sciences (mathématiques, physique, chimie), et apportant donc des compétences clés en cybersécurité, plus de la moitié des acteurs (environ 51,7%) sont des experts du domaine (en tenant compte de celui ayant étudié les deux domaines). En troisième position, la science politique concerne 24,1 % de notre échantillon, soit 7 individus. Ce sont ici des formations en lien avec les affaires européennes et la gouvernance de l'UE. Ainsi, 21 des 29 acteurs (soit 72,4%) sont spécialisés en cybersécurité et/ou en politique européenne, en tenant compte des doubles cursus (ici encore en prenant en compte les acteurs ayant effectué un double cursus).

Ainsi, contrairement à l'agence Eurofound, où la majorité des individus ont suivi des études généralistes (sciences sociales, économie, droit), une partie des membres de l'ENISA semblent avoir acquis une spécialisation dans le domaine régulé par l'agence dès leurs études.

L'analyse croisée des domaines d'études et du genre (cf. graphiques ci-dessous) met en lumière des disparités significatives, en écho aux tendances observées dans la section sur le niveau de diplôme. Comme attendu, les filières scientifiques et techniques restent majoritairement masculines : 100 % des acteurs formés en informatique (9 sur 9) et 6 sur 7 des diplômés en sciences (soit 85,7 %) sont des hommes. Même en tenant compte de leur surreprésentation dans l'échantillon (23 hommes pour 6 femmes), l'écart demeure marqué : 9 hommes sur 23 (soit 39 %) ont une formation en informatique contre aucune femme, et 6 hommes (soit 26 %) ont étudié les sciences, contre seulement 1 femme sur les 6 (17%). À l'inverse, la science politique est plus féminisée, avec 4 des 7 acteurs diplômés qui sont des femmes. Ces chiffres confirment que les hommes sont plus enclins à suivre des cursus scientifiques/techniques, ce qui peut expliquer leur présence numériquement plus élevée dans les postes à responsabilité l'ENISA. Cette tendance est observée au sein d'autres agences comme par exemple avec l'ACER où 37,5% femmes ont fait des études scientifiques, contre 50% des hommes.



Ces résultats s'inscrivent dans une dynamique sociologique plus large, où la répartition genrée des filières scientifiques et techniques reste structurelle. Marianne Blanchard, dans *Genre et cursus scientifiques : un état des lieux*⁵, rappelle que si les femmes progressent en biologie et médecine, elles restent minoritaires en informatique et ingénierie : dans l'OCDE, elles ne représentent que 31 % des diplômés en sciences et ingénierie, contre 64 % en sciences humaines et sociales. Ce phénomène, souvent désigné comme le « *problème du tuyau percé* », traduit l'effet de filtres socio-éducatifs orientant davantage les garçons vers ces disciplines dès le secondaire. De plus, les stéréotypes associant les compétences scientifiques aux hommes influencent négativement le sentiment de légitimité des femmes dans ces domaines.

Ainsi, il est possible de dire que l'ENISA illustre une forme de gouvernement hybride, où l'accès aux fonctions stratégiques et opérationnelles repose sur un équilibre entre expertise technique et compréhension des affaires européennes qui peuvent être acquis dès les études. Cette dynamique pose une question fondamentale : gouverne-t-on parce qu'on maîtrise les arcanes institutionnels de l'UE ou parce qu'on détient un capital régulateur technique propre au domaine en question, ici la cybersécurité ? L'étude des carrières et des expériences professionnelles semble, à ce stade, nécessaire pour poursuivre cette analyse.

e) Carrières et secteur d'expérience professionnelle

- Position européenne au cours de la carrière

14 individus ont travaillé dans les institutions de l'UE à un moment de leur carrière avant de rejoindre l'ENISA, soit 48% de l'échantillon. Ce pourcentage reflète une forte continuité entre les parcours professionnels au sein des structures européennes et les agences spécialisées comme l'ENISA. Une expérience dans les institutions de l'UE permet d'acquérir une compréhension approfondie des cadres réglementaires, compétence directement transférable aux missions de l'ENISA. De plus, travailler au sein d'une agence comme l'ENISA constitue également une continuité logique pour

⁵ Marianne Blanchard, *Genre et cursus scientifiques : un état des lieux*, Revue française de pédagogie, n° 212(3), 109-143, 2021.

les professionnels souhaitant rester dans le cadre institutionnel européen tout en se spécialisant dans des thématiques techniques comme la cybersécurité.

- **Passage dans le privé au cours de la carrière**

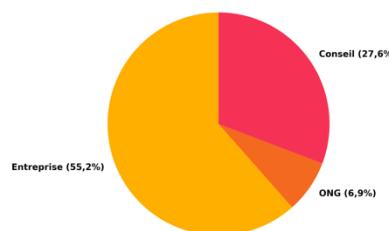
Expérience dans le privé	
OUI	NON
69%	34%

L'ENISA affiche une proportion de 68,97 % de personnel ayant une expérience dans le secteur privé avant d'intégrer l'agence, un taux similaire à celui d'autres agences techniques comme l'ACER (67,74 %), l'EUSPA (75,86 %) ou encore l'AECP (62%). Ce chiffre suggère que l'expérience acquise dans le secteur privé joue un rôle important dans le recrutement à l'ENISA, en particulier pour des domaines techniques comme la cybersécurité. Toutefois, il ne signifie pas préalablement que cette expérience est systématiquement privilégiée, d'autant que l'agence requiert aussi des compétences institutionnelles.

Quantité d'acteurs	Privé (entreprise)	Privé (ONG)	Privé (conseil)
En nombre d'individus	16	2	8
En % du total global	55,2	6,9	27,6

Sur les 29 individus, 55,2 % (16 individus) ont travaillé dans des entreprises privées avant d'intégrer l'ENISA⁶. Cela montre que la majorité des transitions depuis le privé vers l'ENISA proviennent de ce secteur, probablement en raison de compétences techniques ou organisationnelles adaptées au rôle de l'agence. 27,6 % (8 individus) ont travaillé dans le secteur du conseil, indiquant qu'un quart des individus ayant une expérience dans le privé proviennent de ce domaine, souvent lié à des expertises spécifiques ou stratégiques.

Répartition des acteurs ayant travaillé dans le secteur privé (selon les secteurs)



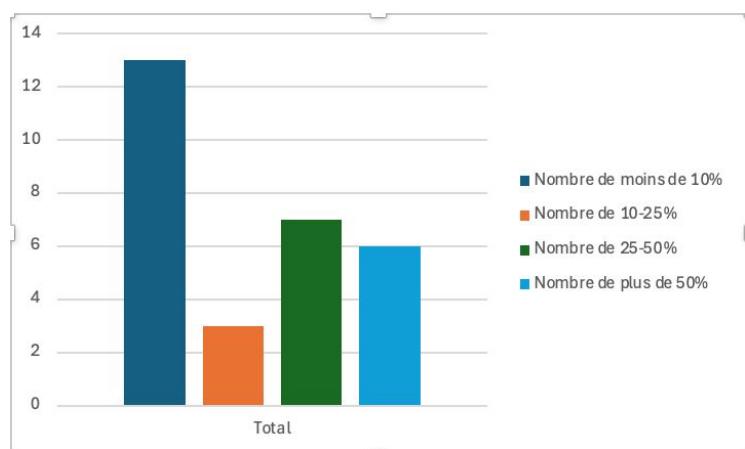
⁶ Voir la liste des entreprises en annexe.

La faible proportion d'individus issus du secteur des ONG (6,9 %, soit 2 personnes) illustre une moindre adéquation entre les missions des ONG et celles de l'ENISA. Dans les agences opérant dans des domaines hautement techniques, comme la cybersécurité, la part des employés ayant une expérience en ONG reste limitée, car ce type de parcours apporte généralement moins d'expertise spécifique par rapport à une expérience en entreprise ou en conseil, et vice versa. Cette tendance se retrouve également dans des agences comme l'Agence européenne pour la propriété intellectuelle ou l'Agence pour la coopération des régulateurs de l'énergie, où la proportion d'employés issus des ONG est très faible. En revanche, dans des agences davantage axées sur des questions sociétales, telles que l'Agence européenne pour l'environnement ou l'Agence européenne pour les conditions de travail, cette proportion est bien plus élevée (jusqu'à 26,67 % pour l'Eurofound)

Part de la carrière passée dans le secteur privé			
-10%	10%-25%	25%-50%	+50%
13 individus	3 individus	7 individus	6 individus

Concernant la part de la carrière passée dans le secteur privé, 13 individus (45 %) ont passé moins de 10 % de leur carrière dans le secteur privé.

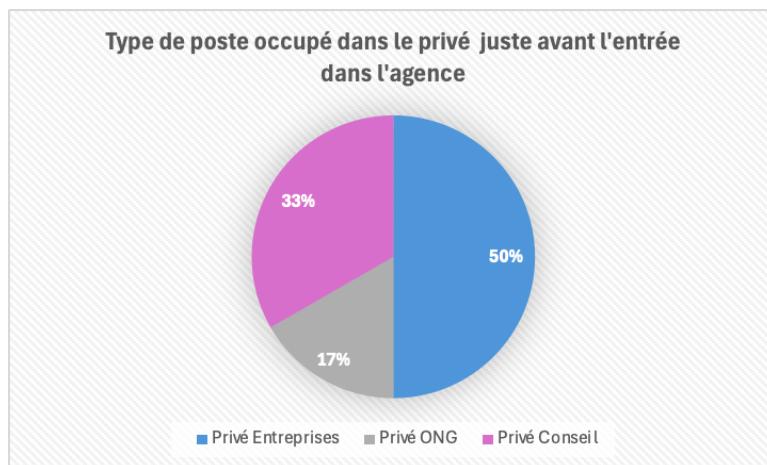
- 3 individus (10 %) ont passé entre 10 % et 25 % de leur carrière dans le privé. Ces profils montrent une familiarité modérée avec le secteur privé avant de rejoindre l'agence.
- 7 individus (24 %) ont passé entre 25 % et 50 % de leur carrière dans le privé, ce qui traduit une expérience plus significative dans ce domaine.
- 6 individus (21 %) ont passé plus de 50 % de leur carrière dans le privé. Ces profils, avec une forte spécialisation dans le privé, sont probablement recrutés pour des compétences pointues.



L'ENISA recrute parmi des profils diversifiés en termes d'expérience dans le secteur privé. Si la majorité des agents a une expérience limitée ou modérée dans ce domaine, une proportion significative (45 % soit 13 personnes) a passé une part importante de sa carrière (plus de 25 %) dans le privé, notamment dans des entreprises ou des cabinets de conseil.

- **Dernière position professionnelle avant d'intégrer l'agence**

Avant d'intégrer l'agence, 21 % des acteurs (6 sur 29) travaillaient dans le secteur privé. Parmi eux, 50 % (3 acteurs) étaient en entreprise, 33 % (2 acteurs) consultants et 17 % (1 acteur) en ONG. Ces chiffres montrent une prédominance des parcours en entreprise, perçue comme un lieu clé de développement des compétences utiles à l'agence. Cela fait écho au résultat précédent selon lequel seuls 6,9% des acteurs ont au moins eu une expérience au sein d'une ONG au cours de leur carrière (avant d'occuper leur poste).



Parmi les acteurs étudiés, 79 % (soit 23 sur 29) occupaient une position professionnelle dans le secteur public juste avant d'occuper leur poste actuel à l'ENISA. Ces données permettent de mener deux analyses complémentaires.

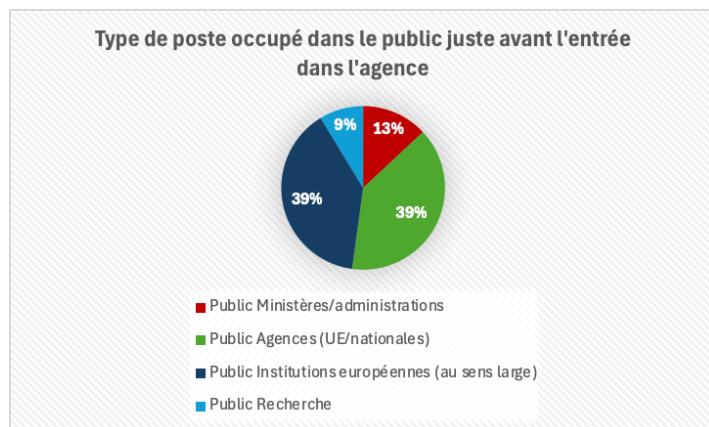
Premièrement, parmi ces 23 acteurs, plus de la moitié (52,2 %, soit 12 individus) occupaient un poste qualifié de « position européenne ». Cela inclut des fonctions exercées au sein d'institutions européennes (au sens large) ou dans des agences européennes. Les 11 autres acteurs (47,8 %) avaient un poste au niveau national, et parmi eux, 39 % (soit 9 personnes) travaillaient au sein d'un ministère, d'une administration ou d'une agence nationale. Ces agences nationales incluent notamment des organismes de cybersécurité, bien que la nature exacte de certaines structures puisse diverger du concept strict d'agence.

Deuxièmement, une analyse par type de structures publiques révèle des résultats particulièrement significatifs. En effet, 9 des 23 acteurs ayant travaillé dans le secteur public (soit 39% et 31% du total de l'échantillon) étaient employés dans une

institution européenne. Ce résultat est assez élevé en comparaison avec certaines agences comme l'EFSA (13%) ou l'Agence européenne des médicaments (17%).

De plus, 9 autres individus occupaient des fonctions régulatrices, dans une agence nationale ou européenne, sur les sujets de cybersécurité (à l'exception de l'un des acteurs ayant travaillé au sein d'Europol). Deux d'entre eux travaillaient déjà à l'ENISA avant d'obtenir leur poste actuel, ce qui souligne une certaine continuité dans leur parcours professionnel.

Ces résultats mettent en lumière que 62%, soit 18 individus de notre échantillon, possédaient, juste avant leur poste actuel, soit une expérience en agence (dont parfois déjà à l'ENISA), soit une expérience au niveau européen. Cela illustre une forte prévalence des trajectoires professionnelles qui s'inscrivent dans des cadres institutionnels ou organisationnels liés à la gouvernance européenne et/ou au enjeux de la cybersécurité.



Pour compléter ces avancées, nous pouvons aussi examiner le type de positions professionnelles occupées par les individus avant leur intégration à l'ENISA. Une tendance assez claire se dégage et vient confirmer ce que nous avançons : la majorité des recrues avaient déjà acquis une expérience notable dans des postes de responsabilité ou d'expertise, ce qui souligne l'exigence de l'agence en termes de qualification et de préparation professionnelle. Ces positions peuvent être regroupées en quatre catégories distinctes.

- Près de la moitié des individus (14 sur 29) occupaient des **postes de leadership**, où ils exerçaient une autorité importante et prenaient des décisions stratégiques. Ces profils, ayant démontré une aptitude à gérer des responsabilités élevées, sont sans doute recherchés par l'ENISA pour leur aptitude à contribuer à la stratégie globale de l'agence.
- Une proportion plus modeste, mais significative (7 sur 29), était engagée dans des **rôles d'expertise ou d'analyse technique**. Ces professionnels possédaient une compétence approfondie dans des domaines spécifiques tels que la cybersécurité ou la protection des données. Bien qu'ils n'aient pas de

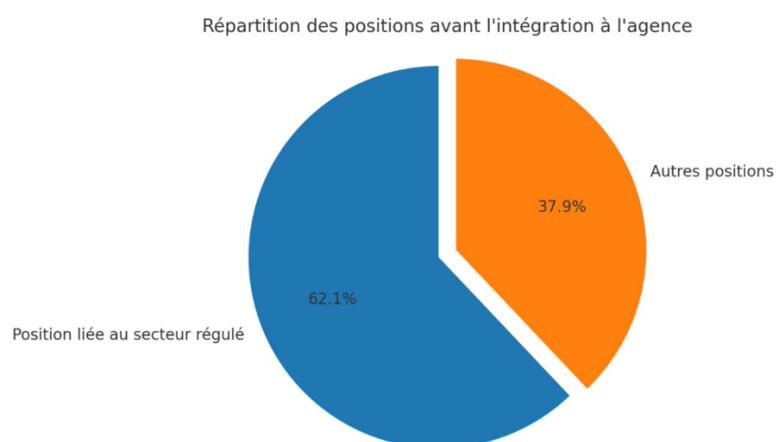
responsabilités de gestion, leur savoir-faire technique et leur capacité à fournir des analyses précises et innovantes font d'eux des atouts précieux dans un environnement hautement spécialisé

- Par ailleurs, 17,20 % (5 sur 29) des individus travaillaient dans des **rôles de gestion de projet ou de management**. Ces postes, souvent situés dans une position intermédiaire entre l'exécution et la supervision stratégique, requièrent des compétences organisationnelles poussées et une aptitude à gérer des initiatives complexes tout en restant alignés avec les objectifs définis par une hiérarchie supérieure. Ce type d'expérience est particulièrement pertinent pour une agence comme l'ENISA, où la coordination entre experts et décideurs est essentielle.
- Enfin, 10,30 % (3 sur 29) des agents provenaient de **rôles de soutien stratégique ou d'adjoints**, des postes impliquant un niveau élevé de responsabilité sans pour autant offrir une autonomie totale. Cela leur a permis de développer une compréhension fine des dynamiques organisationnelles.

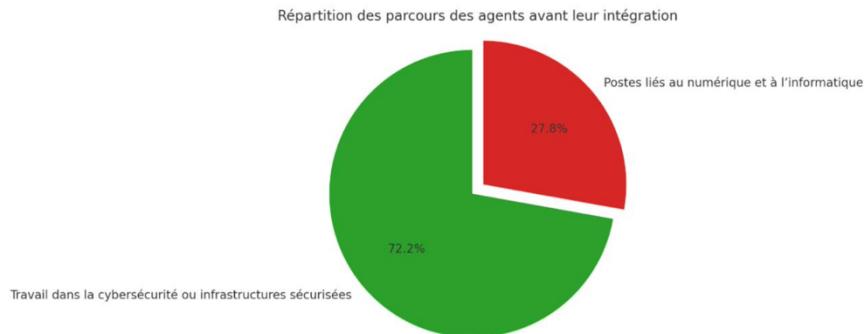
Cette répartition montre que l'ENISA valorise non seulement l'expérience technique et opérationnelle, mais aussi la capacité à évoluer dans des environnements complexes et exigeants. Que ce soit en leadership, en expertise technique ou en gestion de projet, les profils recrutés partagent un point commun : leur capacité à contribuer de manière significative à la mission de l'agence. Cette diversité d'expériences reflète également la complémentarité des rôles nécessaires pour répondre aux défis multiformes de la cybersécurité au sein de l'Union européenne.

- **Ces positions sont-elles en lien avec le secteur régulé ?**

En approfondissant cette analyse, il apparaît que 62,1 % (18 sur 29) des individus étudiés occupaient, juste avant leur intégration à l'agence, une position directement liée au secteur régulé par celle-ci. Cette statistique témoigne de l'importance qu'accorde l'ENISA à recruter des professionnels déjà familiers des thématiques au cœur de sa mission.



On peut décliner cette information de la sorte selon le graphique suivant : une grande majorité de ces acteurs, soit 72,2 % (13 sur 18), travaillait spécifiquement dans le domaine de la **cybersécurité ou de la sécurité des technologies et des infrastructures**. Ces individus possédaient une expertise pointue et une expérience pratique dans la sécurisation des systèmes numériques, des réseaux ou des données, ce qui constitue un atout évident pour une agence comme l'ENISA, dont la mission centrale repose sur ces enjeux. Leur background dans des rôles spécialisés en cybersécurité reflète une adéquation immédiate avec les compétences recherchées pour répondre aux besoins de l'agence. D'un autre côté, 27,8 % de ces agents (5 sur 18) provenaient de postes non directement centrés sur la cybersécurité, mais fortement liés au **numérique et à l'informatique**. Ces rôles, bien qu'éloignés des aspects purement sécuritaires, impliquaient une connaissance approfondie des technologies numériques et de leur fonctionnement, un socle essentiel pour appréhender les problématiques de cybersécurité avec une perspective plus large au sein de l'ENISA.



Ce constat démontre la stratégie de l'ENISA de recruter des professionnels ancrés dans le domaine technologique, qu'il s'agisse de spécialistes en cybersécurité ou d'acteurs du numérique au sens plus large. Cette orientation garantit une base solide de connaissances spécifiques tout en favorisant une diversité de perspectives, indispensable pour appréhender la complexité croissante des enjeux numériques et sécuritaires dans l'Union européenne.

Parmi les 62,1 % précités, 6 proviennent du secteur privé réglementé, ce qui constitue un cas de mobilité direct du secteur privé vers le secteur public pour intégrer l'ENISA. Cela représente alors un facteur de porosité pouvant insinuer la présence du phénomène des portes-tournantes au sein de l'ENISA. Ce phénomène n'est cependant pas observé dans toutes les agences. Par exemple, au sein de l'EFSA, aucun individu de l'échantillon n'avait occupé de poste dans le secteur régulé par l'agence juste avant de l'intégrer. Les enquêteurs ont ainsi souligné que cela indiquait une faible présence du phénomène des portes tournantes au sein cette agence.

Ainsi, à l'ENISA la nature du travail suggère que le recrutement privilégie les compétences spécifiques liées à la régulation et à la cybersécurité, souvent acquises dans le secteur privé ou dans des institutions spécialisées. En effet, les profils des cadres dirigeants montrent que certains ont occupé des postes stratégiques dans des entreprises du secteur technologique ou dans des organismes nationaux de régulation avant de rejoindre l'agence. Ce phénomène de mobilité entre le secteur privé et l'agence reflète une tendance où l'expérience pratique dans la mise en œuvre de normes techniques ou de solutions de cybersécurité est fortement valorisée. Cependant, l'ENISA n'est pas déconnectée de la dimension institutionnelle européenne. Elle fonctionne aussi grâce à des compétences en négociation et une compréhension des mécanismes de gouvernance européenne. Dans ce cadre, des profils combinant expérience technique et savoir-faire institutionnel peuvent donc se démarquer.

f) Mobilités privé-public

Que nous montrent l'ensemble de ces résultats en matière de mobilité public-privé au sein de cette agence ? Si l'on prend en compte toutes ces données, nous pouvons comprendre un élément clé dans l'étude du phénomène des portes tournantes.

	Individus ayant occupé des postes uniquement dans le secteur public avant d'intégrer l'agence	Individus ayant occupé des postes uniquement dans le secteur privé avant d'intégrer l'agence	Individus ayant exercé des mobilités privé-public déjà avant d'intégrer l'agence
Hommes	6	3	14
Femmes	3	1	2
Total	9	4	16
<i>Données intéressantes :</i>			
<i>Sur 23 hommes, 14 ont effectué des mobilités privé-public avant d'intégrer l'agence.</i>			
<i>2 femmes sur 6 ont déjà effectué des mobilités privé-public avant d'intégrer l'agence.</i>			
<i>Sur les 16 individus ayant déjà effectué des mobilités privé-public avant d'intégrer l'agence, on observe que 87,5% (14) d'entre eux sont des hommes contre 12,5% (2) de femmes.</i>			

Ce tableau permet d'analyser les trajectoires professionnelles des individus avant leur intégration à l'agence. On constate que 26,1% des hommes et 50% des femmes n'ont occupé que des postes dans le secteur public avant d'intégrer l'ENISA, soit un total de 9 individus sur 29. Ces personnes ne sont donc pas concernées par le phénomène des portes tournantes, puisque leur carrière s'est exclusivement déroulée dans le public bien que des liens peuvent être établis entre le domaine sur lequel ces

personnes travaillaient et le secteur de régulation de l'agence. En revanche, ces données sont intéressantes car elles signifient que les hommes présentent une plus grande tendance au phénomène de mobilité privé-public.

En ce sens, on observe que 14 hommes sur 23 (60,9%) ont occupé des postes dans le secteur privé et dans le secteur public avant de rejoindre l'ENISA, tout comme un tiers des femmes. Cela suggère que ces individus ont déjà été exposés au phénomène des portes tournantes, ayant déjà évolué entre le secteur public et le secteur privé avant leur arrivée à l'agence. En effet, la part d'homme est ici plus élevée que la part de femmes, ce qui confirme notre précédente hypothèse⁷ et cela peut aussi refléter que les hommes ont plus de dynamiques de carrière et d'opportunités d'emploi dans les secteurs public et privé dans le milieu de la cybersécurité. Ces chiffres s'inscrivent dans la lignée de ce que l'on peut trouver dans d'autres agences. Par exemple, à l'agence de l'Union européenne pour le programme spatial, bien que cette tendance soit plus marquée, il avait été aussi observé qu'un pourcentage d'hommes nettement plus élevé avait effectué des mobilités public-privé.

Enfin, il convient de mentionner les individus qui, tout au long de leur carrière, ont uniquement occupé des fonctions dans le secteur privé (en lien avec les secteurs régulés par l'agence) avant de rejoindre l'ENISA. Ce sont 3 hommes sur 23 et 1 femme sur 6. Ces individus pourraient également être considérés comme ayant contribué au phénomène de mobilité public-privé, à partir du moment où ils ont intégré l'agence après avoir travaillé dans le secteur privé, ce qui soulève des questions sur les liens entre les secteurs public et privé.

IV/ CONCLUSION

L'analyse prosopographique de notre échantillon de 29 individus occupant des postes à responsabilité au sein de l'ENISA met en lumière un mode de gouvernance hybride, où coexistent deux profils dominants (en prenant en compte le type d'études suivi et la carrière professionnelle précédant leur poste à l'ENISA). D'une part, des experts techniques en cybersécurité, majoritairement issus du secteur privé ou d'agences nationales, disposant d'une expertise pointue et directement applicable aux missions de l'ENISA. D'autre part, des individus ayant acquis un capital institutionnel au sein des structures européennes, apportant une maîtrise des règles et dynamiques de l'UE. Cette dualité questionne donc la nature du pouvoir au sein de l'agence : gouverne-t-on à l'ENISA par maîtrise des rouages institutionnels ou par la spécialisation technique accumulée dans le domaine de la cybersécurité ? Notre analyse montre que la gouvernance de l'ENISA repose sur une articulation entre ces deux formes de pouvoir. La technicité est indispensable à la compréhension et à la mise en œuvre des politiques de cybersécurité, mais elle ne saurait suffire à elle seule

⁷ Sarah Kolopp, "Pantoufle, une affaire d'hommes ? Les énarques, l'administration financière et la banque (1965-2000)", *Sociétés contemporaines*, 2020. <https://www.cairn.info/revue-societes-contemporaines-2020-4-page-71.htm>

dans un environnement institutionnel européen complexe. Ainsi, les profils combinant une expertise technique et une expérience institutionnelle tendent à occuper des positions stratégiques. En ce sens, le pouvoir à l'ENISA ne se construit pas sur une opposition entre institutionnalisation et technicité, mais sur une synergie entre ces deux dimensions.

Par ailleurs, d'un point de vue sociologique, notre échantillon révèle une surreprésentation des hommes, notamment dans les fonctions à responsabilité 'technique'. Cette étude montre donc que les domaines scientifiques restent encore aujourd'hui des environnements très masculin.

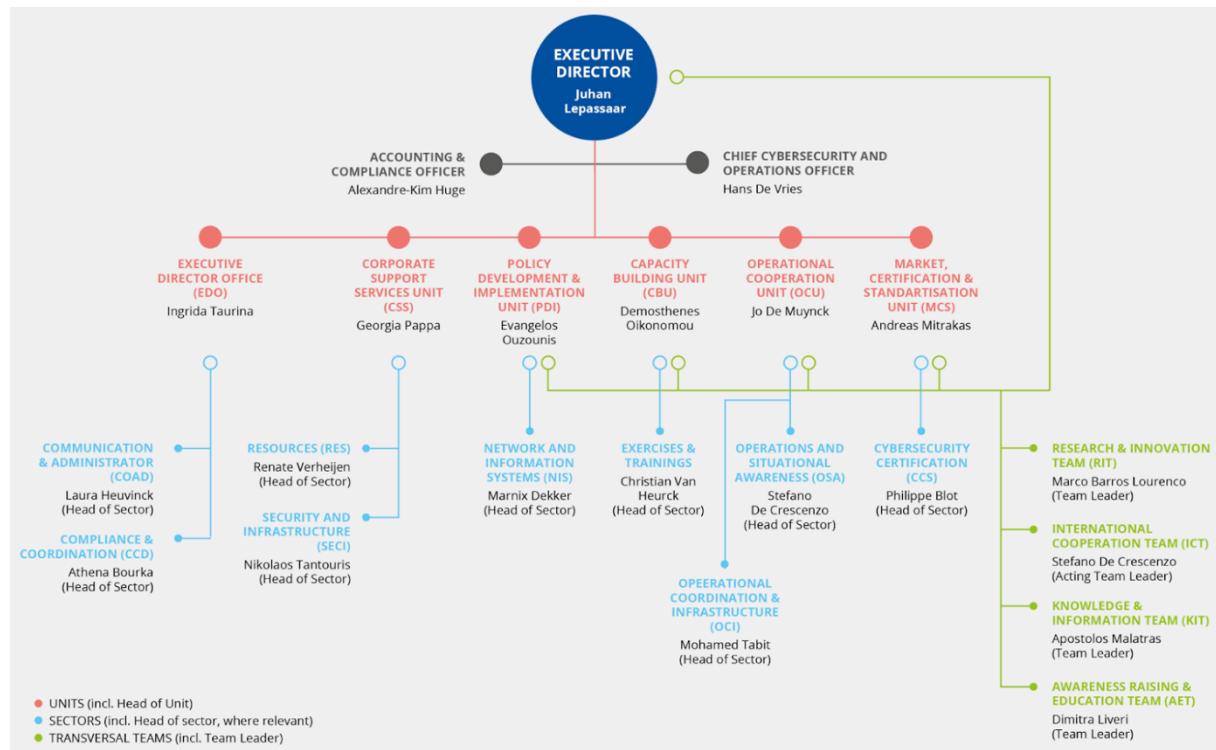
Le phénomène des « portes tournantes » semble présent au sein de l'ENISA. L'analyse révèle que 6 des 29 acteurs occupaient, juste avant leur fonction actuelle au sein de l'agence, un poste dans le secteur privé régulé par celle-ci. Plus encore, on constate que 16 individus ont effectué des mobilité public-privé sur l'ensemble de leur carrière avant l'ENISA, transitant entre des fonctions de régulateurs en cybersécurité (secteur public, tant au niveau européen que national, et des postes dans le secteur privé régulé (conseil et entreprises). Ces résultats font écho aux analyses menées sur l'agence de l'UE pour le programme spatial (EUSPA) et sur l'agence européenne de contrôle des pêches (AECP), qui elles aussi semblent être sujettes au phénomène des "portes tournantes". Toutefois, c'est un phénomène à nuancer, puisque plusieurs des agences européennes ne semblent pas (ou dans une moindre mesure) concernées par cette mobilité public-privé, en lien avec le secteur régulé (EFSA, ACER (cas particulier de la structure du secteur de l'énergie), Eurofund). Si cette porosité entre les secteurs à l'ENISA peut renforcer l'expertise de l'agence, elle interroge néanmoins sur l'influence potentielle des intérêts privés dans la prise de décision et soulève des préoccupations quant aux risques de conflits d'intérêts dans la gouvernance de celle-ci.

Un autre point de vigilance concerne la transparence des déclarations d'intérêts des membres de l'agence. Si certaines obligations de publication existent, elles restent limitées, et le manque d'accessibilité à ces documents (sauf pour les individus ayant des postes à très haute responsabilité), restreint la possibilité de vérifier d'éventuels conflits d'intérêts et nuit à la prévention des risques de capture réglementaire.

Enfin, il convient de replacer ces résultats dans le cadre des limites de notre recherche. Fondée sur un échantillon de 29 personnes, notre étude ne peut prétendre à une représentativité absolue des dynamiques de gouvernance au sein de l'agence. De plus, comme mentionné, la fiabilité des informations repose largement sur des sources indirectes, pouvant contenir des biais ou omissions. En conséquence, et en gardant à l'esprit ces limites, notre analyse offre une première approche des dynamiques de pouvoir à l'ENISA, appelant à des recherches complémentaires pour affiner la compréhension des interactions entre expertise, institutions et intérêts privés dans la gouvernance européenne de la cybersécurité.

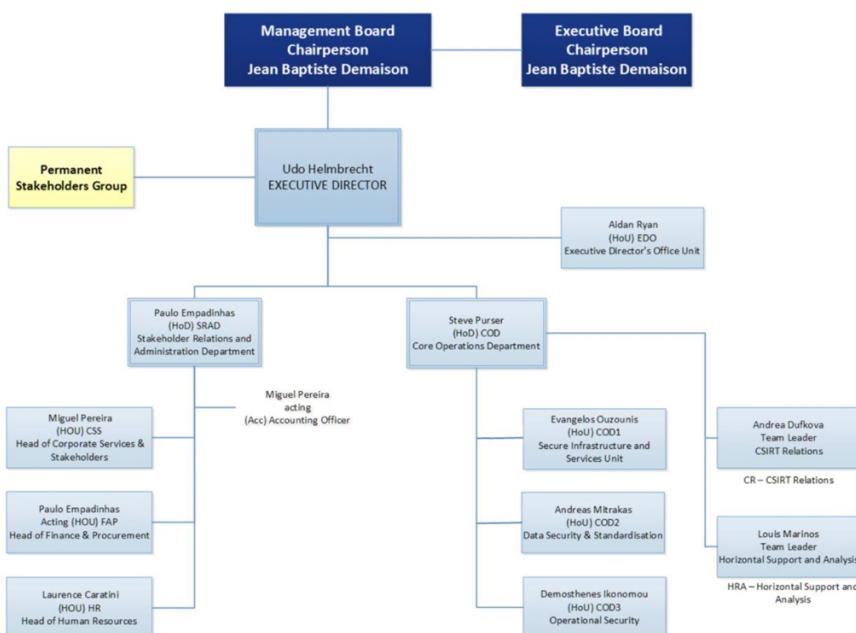
Annexes

Organigramme actuel (décembre 2024)



Ancien organigramme

Cet organigramme a été obtenu grâce à Internet Archive sur une version du site internet de l'ENISA de 2017.



Liste des entreprises dans lesquelles les individus ont travaillé

PwC Luxembourg
KPMG Luxembourg
Liberty Ermitage
HSBC Securities
Premium Select Lux SA
Vroom & Dreesmann Nederland BV
CAOP
IEKEP
City University
APM Terminals
Fraunhofer FOKUS
GlobalSign
Verizon Business
Thales Research and Technology
Cloud Security Alliance
PETA AE
NCC Group Europe - Fox-IT B.V.
SecuraSecura
EXIN
EY (ancien nom Ernst & Young)
Philips Industrial Electronics
DFM Développement formations métiers
Messerschmitt-Bölkow Blohm GmbH Munich
Télécom ParisTech
Cisco
Nask
Société Générale
Alpha Bank
Emirec
Tracy International
Grande Consumo
Liscic-Toshiba
Genesy SRL
TNO Information and Communication Technology
KPMG Netherlands
CultuurNet Vlaanderen
Logica
Cetrel s.c.
Cartermill International
Banque Générale du Luxembourg
Clearstream
Hamilton Stock Brokerage
GMD
Siz GmbH Bonn
IICS GmbH
Mnemon

Exemple d'une déclaration d'intérêts : celle de Juhani Lepassaar, Directeur exécutif



EUROPEAN UNION AGENCY
FOR CYBERSECURITY

Agamemnonos 14
Chalandri 15231 | Attiki | Greece
Tel: +30 28 14 40 9711
E-mail: info@enisa.europa.eu
www.enisa.europa.eu

ANNUAL DECLARATION OF INTEREST

Title (Ms., Mr., Dr., Prof.) *Mr*

First Name: *Julian*

Surname: *Lepanias*

ENISA Position: *Executive Director*

hereby declares to have the following direct or indirect interest of relevance to ENISA:

1. Work and activities in organisations relevant to the operating area of ENISA.

During the past 3 years, all activities performed for or on behalf of an organization operating in a related field, whether related to the substance of ENISA mandate or to its operational support, and whether or not these activities have been subject to regular or occasional remuneration in cash or kind, either by the declaring member or to the best of his/her knowledge the members of his/her household, including: i) participation in the internal decision-making of a company (e.g. Board membership, executive or non-executive directorship), ii) permanent or temporary member of the personnel of a company/institute (Other activities performed within a company (e.g. traineeship) are also subject to declaration.), iii) work contracted out by companies/institute, through consultancy or otherwise.

Indicate names of organisation/Position/Period:

none

2. From the moment of taking the post of the member on relevant statutory body of ENISA, any financial interests, in a company relevant to the operating area of ENISA and/or voting rights in a company, including holding of stocks and shares, equity, bonds, partnership interests¹ in the capital of a company, one of its subsidiaries or a company in the capital of which it has a holding (names of the companies):

none

¹ When declaring financial interests e.g. stocks and shares, only the kind, number and company name need be stated.



3. Other links with the field of activity of ENISA during the preceding 3 years, including the participation in relevant activities supported by EU grants or contracts. All assistance and support received from stakeholders of ENISA, whether associated with direct or indirect pecuniary or material benefits, including: i) grants for study or research, ii) fellowships or sponsorships endowed by a company operating in the related business and iii) any other relevant activity related to EU grants and contracts. If such assistance or support is still subject to compensation in any form then declaration of any activity independently of granting period:

None

4. Any membership role or affiliation, or any other links with the organisations relevant to ENISA.

During the preceding 3 years, interests of non-pecuniary or material benefit to the declaring member, arising from professional activities or affiliation with national or international organisations or bodies with tasks similar to ENISA. It also includes the participation in public interest groups, professional societies, clubs or organisations which have an agenda or an interest or involvement in ENISA's work:

None

4. Other interests or facts whether or not related to such organisations which you consider should be made known to ENISA, including matters relating to the members of your household:

My spouse works as a Head of Cabinet
of the Member of the European Court of
Auditors

I hereby declare that I have read the MB Decision for prevention and management of conflicts of interest and that the above Declaration of Interest is at my knowledge complete.

I further declare that should any changes occur and should it appear that I have or acquire additional interests that should be made known to ENISA I shall forthwith declare them and complete a new declaration of interests detailing the changes.



I understand that this Declaration will be entered in a register held by the Agency, and will be accessible to the public, on request, at the headquarters of the Agency and will be made public on the Agency's website.

Please note that the European Union Agency for Cybersecurity (ENISA) will ensure on its part that your personal data hereby submitted is processed as required by *Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data*. The purpose of processing this data is to safeguard the independence of ENISA's advice, clarify its credibility as a body of expertise, and to protect the brand value of ENISA and its constituent bodies. To this end, your Declaration of Interest will be publicly accessible upon request and will also be made available at ENISA's website for reasons of transparency. ENISA will make any possible effort to remove any potential sensitive data from the public version of your Declaration of Interest, unless this is not possible in the context of the pursued purpose. ENISA will not keep any Declaration of Interests for a period longer than 5 years after the end of your mandate.

You have the right of access to your personal data and to relevant information concerning how we use it. You have the right to rectify your personal data. Under certain conditions, you have the right to ask that we delete your personal data or restrict its use. You have the right to object to our processing of your personal data, on grounds relating to your particular situation, at any time. We will consider your request, take a decision and communicate it to you.

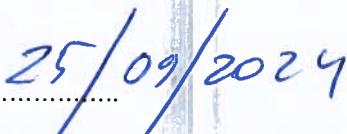
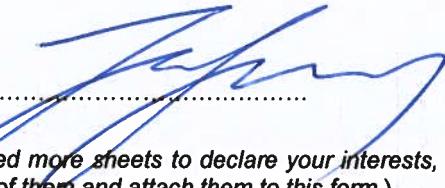
In case in the Declaration of Interest you include information about other data subjects (i.e. your family), you are requested to inform them about this fact and provide them with access to the relevant information.

If you have any queries concerning the processing of your personal data, you may address them to the Secretariat of the respective statutory body. You may also contact at any time the ENISA DPO at dataprotection@enisa.europa.eu.

You have the right of recourse at any time to the European Data Protection Supervisor at <https://edps.europa.eu>.

Signature:.....

Date:.....

A handwritten signature in blue ink is written over the signature line. To its right, a handwritten date "25/09/2024" is written vertically along the line.

(If you need more sheets to declare your interests, do not hesitate to use blank ones, but please sign each one of them and attach them to this form.)