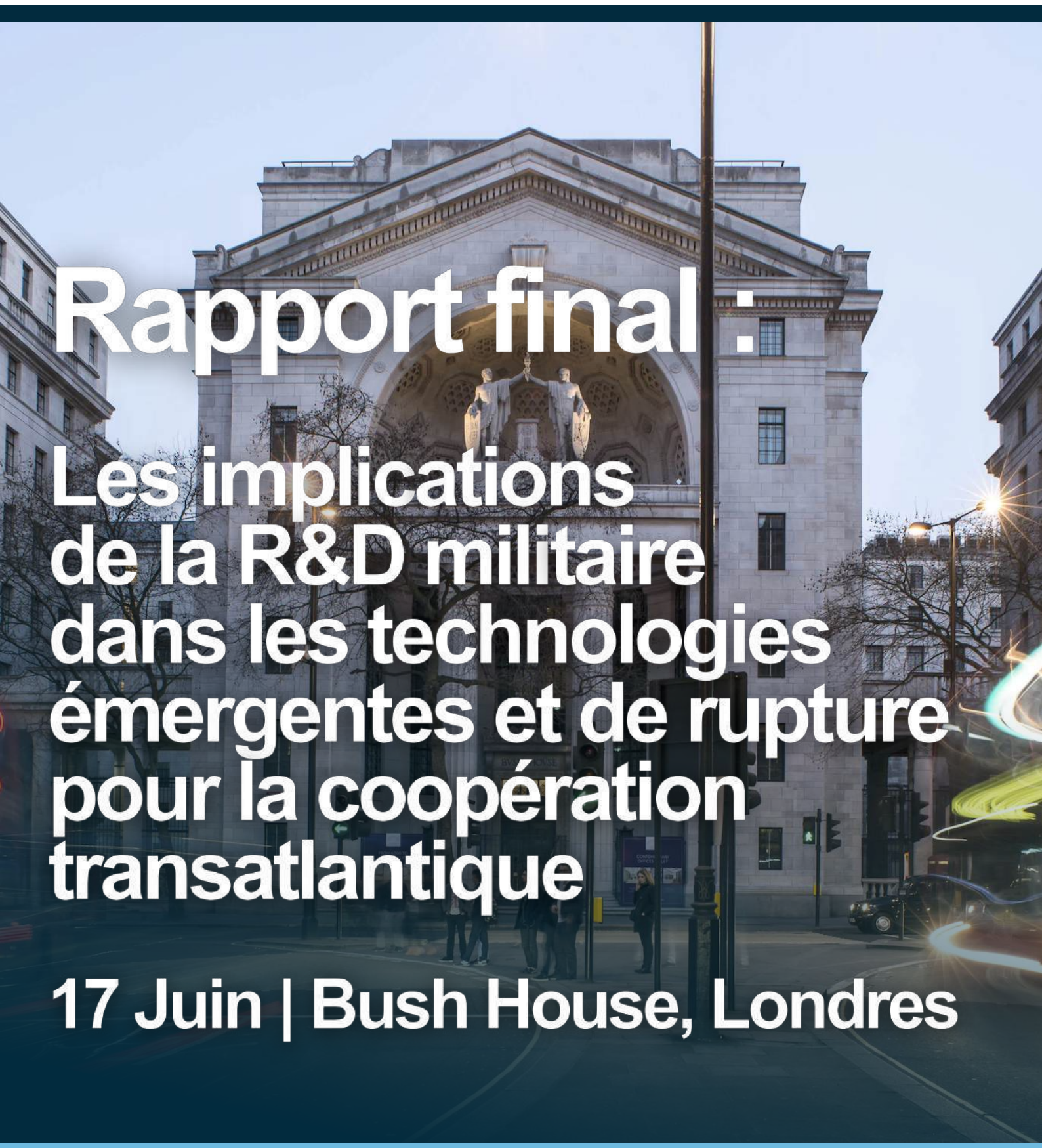


Rapport final :

Les implications de la R&D militaire dans les technologies émergentes et de rupture pour la coopération transatlantique

17 Juin | Bush House, Londres

M. Bekkers, A. Bumpers, R. Csernatoni, S. Daultrey, K. Floyd,
T. Lawrence, T. Longo, E. Marcus, P. Pernik, K. Tucker

Les implications de la R&D militaire dans les technologies émergentes et de rupture pour la coopération transatlantique

Authors: M. Bekkers, A. Bumpers, K. Tucker
Editors: R. Csernatoni, S. Daultrey, K. Floyd, T. Lawrence, T. Longo, E. Marcus, P. Pernik

WILLIAM & MARY
CHARTERED 1693
CCDCOE
NATO COOPERATIVE CYBER DEFENCE CENTRE OF EXCELLENCE
UNITED STATES MISSION
NORTH ATLANTIC TREATY ORGANIZATION
CARNEGIE EUROPE
KING'S College LONDON

Table des matières

Avant-propos

La divergence des visions et des stratégies d'innovation technologique militaire entre les États-Unis et les pays membres de l'OTAN, en particulier en Europe, a un impact significatif sur la coopération transatlantique. Alors que les technologies émergentes et de rupture (EDT) - telles que l'IA, l'informatique quantique et la robotique avancée - façonnent de plus en plus la sécurité mondiale, les approches concurrentes de la R&D à double usage et militaire au sein de l'Alliance transatlantique créent des défis pour l'élaboration de politiques cohérentes et les efforts conjoints d'innovation. Les États-Unis et l'Europe ont des priorités, des mécanismes de financement et des objectifs stratégiques différents, ce qui peut entraîner des désalignements dans la manière dont les technologies sont développées, déployées et intégrées dans les opérations militaires. Dans le contexte d'un paysage géopolitique en évolution et de la guerre russo-ukrainienne en cours, cette divergence pose des risques pour l'efficacité de la coopération transatlantique en matière de défense et de sécurité.

Cet atelier d'une journée a examiné des visions concurrentes de l'innovation technologique militaire, en se concentrant sur la manière dont celles-ci influencent les politiques d'innovation industrielle et technologique des deux côtés de l'Atlantique. En dévoilant les différences et les points communs, les participants de l'armée, du gouvernement, de l'industrie, des universités et d'autres ont identifié des opportunités d'alignement et de collaboration accrus, contribuant à une coopération militaire transatlantique plus cohérente et efficace.

Cet atelier était la prochaine étape d'un partenariat approfondi et durable entre le Centre d'excellence pour la cyberdéfense en coopération (CCDCOE), le King's College de Londres et Carnegie Europe, avec le soutien de la Mission des États-Unis auprès de l'OTAN. Financé par la Mission américaine auprès de l'OTAN, William & Mary, le CCDCOE et le King's College de Londres ont publié « Cyber Threats and NATO 2030: Horizon Scanning and Analysis » (Les cybermenaces et l'OTAN en 2030 : veille stratégique et analyse) en 2020. Nous avons ensuite organisé un événement virtuel jusqu'à ce que nous puissions nous réunir en octobre 2022 à Bruxelles pour un atelier sur la cyber-résilience, cette fois avec Carnegie Europe. À chaque étape, nous avons répondu à l'appel de la Mission des États-Unis auprès de l'OTAN pour nous appuyer sur des idées et des approches novatrices et aller de l'avant pour en faire plus.

Cette publication contient un résumé des débats et des principaux résultats obtenus par les groupes de discussion. Pour permettre un maximum de discussions et de débats, la majorité de l'atelier a fonctionné selon la règle de Chatham House sans attribution.

En tant que leader mondial dans le domaine de l'éducation, William & Mary est profondément reconnaissant à ses hôtes, à ses collaborateurs et à la mission des États-Unis auprès de l'OTAN de lui avoir donné les moyens de contribuer à rendre le monde plus sûr.

Kathryn H. Floyd, Ph.D.
Directrice
Whole of Government Center of Excellence

Prof. Teresa V. Longo, Ph.D.
Responsable senior
des relations internationales

Horaires des ateliers

9 h 00 – 9 h 10	**Discours de bienvenue** Prof. Teresa V. Longo, Responsable senior des relations internationales, William & Mary Dr. Kathryn H. Floyd, Directrice, Whole of Government Center of Excellence, William & Mary
9 h 10 – 9 h 30	**Discours d'ouverture** Rodney D. Ford, Ministre conseiller aux affaires publiques, Mission des États-Unis au Royaume-Uni
9 h 30 – 10 h 30	**Panel plénier - « La concurrence géopolitique en EDT : Implications pour l'OTAN et les rivalités technologiques »** Fiona Bradley, Cheffe de cabinet, Défense, Palantir Technologies Dr. Joe Devanny, Professeur associé, National Security Studies, Department of War Studies, King's College London Dr. Amy Ertan, Responsable des politiques cybernétiques et hybrides, Siège de l'OTAN Piret Pernik, Chercheur, Division stratégie, Centre d'excellence pour la cyberdéfense en coopération de l'OTAN
10 h 30 – 10 h 45	**Pause café**
10 h 45 – 12 h 45	**Groupe de discussion 1 : « Visions concurrentes des EDT militaires »** Professeur Antonio Calcara, Chargé de recherche principal, Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussels Dr. Raluca Csernatoni, Boursière, Carnegie Europe Dr. Edward Hunter Christie, Enseignant chercheur senior, Finnish Institute of International Affairs Dr. Simona Soare, Professeure associée, Lancaster University

10 h 45 - 12 h 45	**Groupe de discussion 2 :** **« Domaines d'alignement de ces visions concurrentes »** KatyAnn Coulter, Responsable, Data Programs Branch ACC A29P, ACC/A29 Data Tech Futures Division, United States Air Force Benjamin Dunlap, Chef de la direction des opérations de données, United States Air Force/Air Combat Command/A29 Dr. Nathan Fisher, Chef de la direction des opérations de données, Noblis, Inc. Dr. Kathryn H. Floyd, Directrice, Whole of Government Center of Excellence, William & Mary Huw Williams, Boursier senior et éditeur, The Military Balance, The International Institute for Strategic Studies
10 h 45 - 12 h 45	**Groupe de discussion 3 : « Partage de renseignements sur les cybermenaces entre les alliés de l'OTAN »** Eman Blair, Vice-Président principal pour l'avancement de la technologie et Conseiller spécial, Pentagon Federal Credit Union Sally Daultrey, Chercheuse associée, Whole of Government Center of Excellence, William & Mary Dr. Andrea Gilli, Maître de conférences, Université de Saint Andrews Roger Yee, Associé principal, Outcome One
13 h 45 – 14 h 15	**Rapport des groupes de discussion**
14 h 15 - 14 h 30	**Remarques de clôture** Dr. Kathryn H. Floyd, Directrice, Whole of Government Center of Excellence, William & Mary

Coanimateurs de l’atelier

WILLIAM & MARY
CHARTERED 1693

UNITED STATES MISSION
NORTH ATLANTIC TREATY ORGANIZATION

KING'S College LONDON

CCDCOE
NATO COOPERATIVE
CYBER DEFENCE
CENTRE OF EXCELLENCE

CARNEGIE
EUROPE

Collaborateurs de l’atelier

PS21
PROJECT
FOR THE STUDY OF THE
21ST CENTURY

YOUNG PROFESSIONALS IN FOREIGN POLICY

YOUNG PROFESSIONALS
IN FOREIGN POLICY

Biographies des auteurs

Myrthe Bekkers

Myrthe Bekkers est étudiante en master National Security Studies au King's College London. Elle est assistante de recherche au Freeman Air and Space Institute de la School of Security Studies, où elle contribue à une analyse axée sur les politiques de la dynamique d'escalade dans l'espace. Ses propres recherches portent sur l'autonomie stratégique et les capacités spatiales néerlandaises dans les Forces armées, l'autonomie maritime et les technologies de rupture dans la défense.

Myrthe est titulaire d'un BA en Relations internationales et organisation internationale et d'un BA en Droit néerlandais de l'Université de Groningue, et apporte son expérience en droit commercial et en recherche sur les politiques.

Alex Bumpers

Alex Bumpers est étudiant en master au sein du programme Intelligence and International Security au King's College de Londres (KCL). Ses études examinent l'intersection des technologies émergentes et de la sécurité. Il s'intéresse particulièrement à la cyberdéfense et aux partenariats d'innovation public-privé. Auparavant, il était consultant senior dans le cadre de la pratique Guidehouse's defence and Security, où il dirigeait des projets d'innovation en matière de sécurité nationale pour des clients fédéraux axés sur la gestion des risques et la résilience nationale. Avant cela, il a soutenu des projets de transformation numérique au Département d'État américain. Il a obtenu son BA en Histoire des politiques publiques de l'Université de Californie à Santa Barbara.

Dr. Raluca Csernatoni

Raluca Csernatoni est enseignante chercheuse. Elle travaille sur la sécurité et la défense européennes avec un accent sur les technologies émergentes et de rupture comme l'Intelligence artificielle (IA), à Carnegie Europe à Bruxelles, en Belgique. Chez Carnegie Europe, elle est cheffe d'équipe et experte en recherche senior sur les nouvelles technologies pour le projet EU Cyber Diplomacy Initiative - EU Cyber Direct (EUCD) et dirige les recherches de Carnegie Europe sur « La technopolitique de l'IA de l'UE ». Csernatoni est actuellement professeure en sécurité et défense européennes, spécialisée dans les technologies numériques, au sein de la Brussels School of Governance (BSoG) et de son Centre for Security, Diplomacy and Strategy (CSDS) à la Vrije Universiteit Brussel (VUB), en Belgique. Au CSDS, elle est également experte senior en recherche sur les technologies numériques dans le cadre du projet financé par l'Union européenne « Indo-Pacific-European Hub for Digital Partnerships: Trusted Digital Technologies for Sustainable Well-Being - INPACE ».

Sally Daultrey

Sally Daultrey est collaboratrice de recherche au Whole of Government Centre of Excellence de l'Université William & Mary, où elle travaille en collaboration avec la professeure Chon Abraham sur l'analyse comparative des cadres, lois et pratiques en matière de partage de renseignements sur les cybermenaces aux États-Unis et dans d'autres juridictions. Avec 22 ans d'expérience sur le terrain dans 29 pays, elle a beaucoup travaillé en Asie centrale, en Inde, à Singapour et aux États-Unis sur la diplomatie scientifique et des projets de sécurité non traditionnels. Elle est basée à Londres.

Dr. Kathryn H. Floyd

Kathryn H. Floyd, Ph. D. est directrice du Whole of Government Center of Excellence (WGC) de l'Université William & Mary. Le WGC, qui fait partie du programme Veteran-to-Executive Transition (W&M VET) de l'Université William & Mary, sert de pôle universitaire dédié à toutes les questions de sécurité nationale : formation militaire et inter-agences, développement du leadership stratégique, mise en réseau entre universitaires et praticiens autour des priorités de recherche, et enseignement diplômant.

Floyd a obtenu son doctorat en études stratégiques (avec un focus sur la pré-radicalisation) à la S. Rajaratnam School of International Studies de la Nanyang Technological University (Singapour), où elle a travaillé avec l'International Centre for Political Violence and Terrorism Research (ICPVTR). Elle est titulaire d'un master en Études sur la guerre du King's College de Londres (Royaume-Uni) et d'un B.A. en Sciences politiques de l'Université William & Mary.

Tyler Lawrence

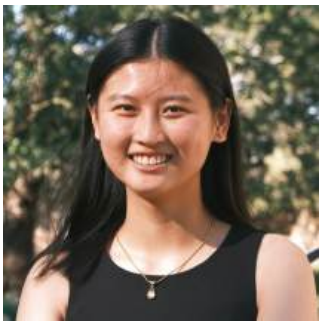
Tyler Lawrence est responsable des événements internationaux au Reves Center for International Studies de l'Université William & Mary. Dans son rôle, il planifie et gère des événements internationaux sur le campus et à l'étranger pour aider à cultiver une université mondiale. Avant William & Mary, Tyler a travaillé dans la gestion d'événements théâtraux et cinématographiques à New York. Il est titulaire d'un BA en Anglais obtenu à l'Université George Mason, ainsi que d'un Master en Éducation (M.Ed.) délivré par l'Université Old Dominion.

Prof. Teresa Longo

Dr Teresa Longo est vice-provost associée aux affaires internationales et directrice exécutive du Reves Center for International Studies à l'Université William & Mary. Elle est également professeure d'études hispaniques. Elle est titulaire d'un doctorat de l'Université du Wisconsin-Madison et d'un M.A. et d'un B.A. de l'Université du Montana. Sa bourse se concentre sur la relation entre l'Amérique latine et les États-Unis telle qu'elle est articulée culturellement.

Les publications du professeur Longo incluent une dissidence visible : Latin American Writers, Small U.S. Presses, and the Political Imagination ; « Humanity Rendered Visible : Literature, Art and the Post-9/11 Imagination » ; et Pablo Neruda and the US Culture Industry.

Elle est récipiendaire du prix Thomas Jefferson de William & Mary, d'un Jefferson Teaching Award, d'un Alumni Society Teaching Award et d'un Plumeri Award ; elle a été reconnue par la Case-Carnegie Foundation comme professeur de Virginie de l'année.

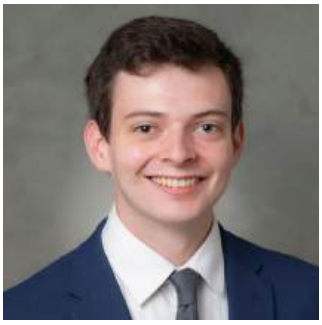


Elizabeth Marcus

Elizabeth Marcus est une étudiante de 4e année à William & Mary avec une spécialisation en Relations internationales et philosophie. Elle est coprésidente du William & Mary Global Innovation Challenge(WMGIC), une organisation dirigée par des étudiants qui organise des concours de cas interdisciplinaires et mobilise les jeunes adultes pour s'attaquer aux problèmes mondiaux de sécurité et de développement durable. En tant que boursière Freeman à l'Université William & Mary, Elizabeth effectue actuellement un stage au sein du Caucus of Development NGO Networks (CODE-NGO), situé à Quezon City, aux Philippines. Après l'obtention de son diplôme, Elizabeth espère servir son pays à l'étranger au Département d'État américain.

Piret Pernik

Piret Pernik est chercheuse au sein de la Division Stratégie du Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE) Elle est également doctorante au Département des technologies militaires de l'Université de la Défense nationale, en Finlande, depuis 2024. Elle travaille dans le domaine de la cybersécurité depuis 2013 en tant que chercheuse et a rédigé et co-rédigé de nombreux rapports de recherche et analyses de politiques, y compris des chapitres de livres, et publiés dans des revues scientifiques à comité de lecture. Avant de rejoindre le CCDCOE en 2019, Piret Pernik était enseignante chercheuse au sein de l'International Centre for Security and Defence (ICDS), le plus grand groupe de réflexion d'Estonie axé sur les questions de sécurité et de défense. Entre 2003 et 2013, elle a travaillé au ministère estonien de la Défense dans la section de planification de la politique de défense. Elle a travaillé pendant trois ans en tant que conseillère de la Commission de la Défense nationale du Parlement estonien de 2009 à 2012. Elle est titulaire d'un master en Théorie sociale (sociologie) obtenu à l'Institut estonien des humanités de l'Université de Tallinn, ainsi que d'un master en Relations internationales et études européennes délivré par l'Université d'Europe centrale à Budapest.



Kyle Tucker

Kyle Tucker est titulaire d'une bourse Marshall et poursuit des études supérieures en sécurité nationale et stratégie au King's College de Londres et à l'Université de St Andrews. Son orientation académique et professionnelle est axée sur la sécurité internationale, en particulier les questions nucléaires et la politique scientifique et technologique. Auparavant, il a œuvré au programme Scoville Peace Fellow à la Nuclear Threat Initiative à Washington, DC, et comme stagiaire au Center for Nonproliferation Studies à Monterey, en Californie. Ancien boursier Boren, il a également étudié la langue russe à Almaty, au Kazakhstan. Tucker est titulaire d'un BA en études internationales et en russe de l'Université de l'Indiana à Bloomington et est un fier Hoosier.

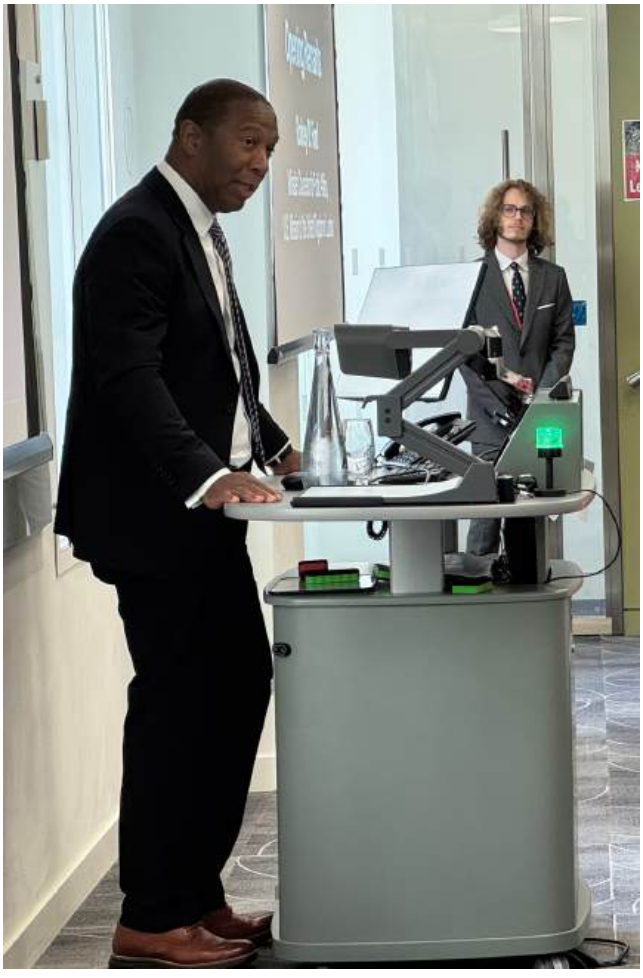
Discours d’ouverture

Discours d'ouverture

Rodney D. Ford, Ministre conseiller pour les affaires publiques,
Mission des États-Unis au Royaume-Uni

Rodney D. Ford, Ministre conseiller pour les affaires publiques à la Mission des États-Unis au Royaume-Uni, a prononcé le discours d'ouverture de l'atelier. M Ford a ouvert la session en soulignant l'importance du Sommet de l'OTAN de 2025 à La Haye et le besoin urgent pour l'OTAN d'améliorer la coopération militaire et de favoriser l'innovation en réponse à l'évolution actuelle de l'environnement de sécurité. Il a souligné l'ingéniosité des forces ukrainiennes, qui tirent parti d'une combinaison de solutions de haute et de basse technologie pour remodeler le champ de bataille. M Ford a souligné la nécessité d'anticiper les évolutions de la guerre, plutôt que d'y réagir, en tirant les leçons des champs de bataille actuels et en déployant les technologies émergentes et de rupture (EDT) afin de renforcer la dissuasion et d'élargir le spectre des options en matière de sécurité.

M Ford a insisté sur le fait que l'OTAN devait évoluer pour demeurer l'alliance militaire la plus performante au monde. Il a souligné l'importance des investissements dans la défense collective, saluant les plus de 20 alliés qui ont augmenté leurs dépenses depuis septembre 2024. Il a fait valoir qu'il était nécessaire de porter les engagements en matière de dépenses de défense à 5 % du PIB pour garantir que l'innovation se traduise en capacités réelles. Il a appelé à une augmentation des investissements dans les technologies émergentes et perturbatrices, soulignant l'importance d'accélérer l'innovation et de l'intégrer grâce à une rationalisation de l'acquisition et du déploiement de la défense. Des munitions aux micropuces, il a défendu une coopération industrielle transatlantique plus approfondie et un effort unifié à travers les secteurs et les frontières. En conclusion, le message était clair : L'OTAN doit diriger, et non suivre, en évoluant pour répondre aux réalités des conflits modernes.



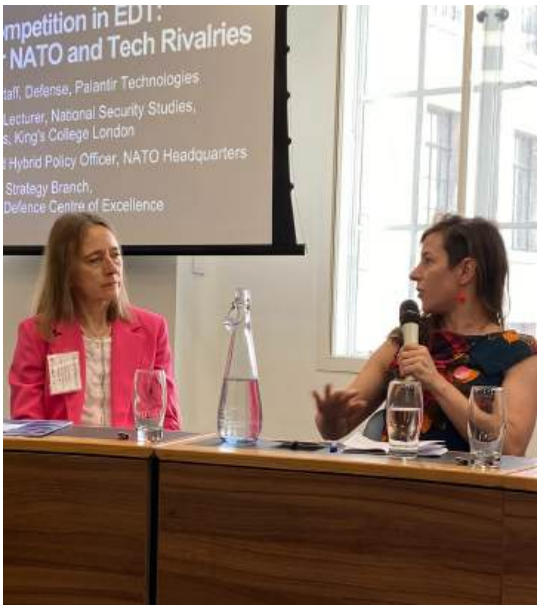
Panel plénier

Compétition géopolitique en EDT : Implications pour l'OTAN et les rivalités technologiques

Panel plénier - « La concurrence géopolitique en EDT : Implications pour l'OTAN et les rivalités technologiques »

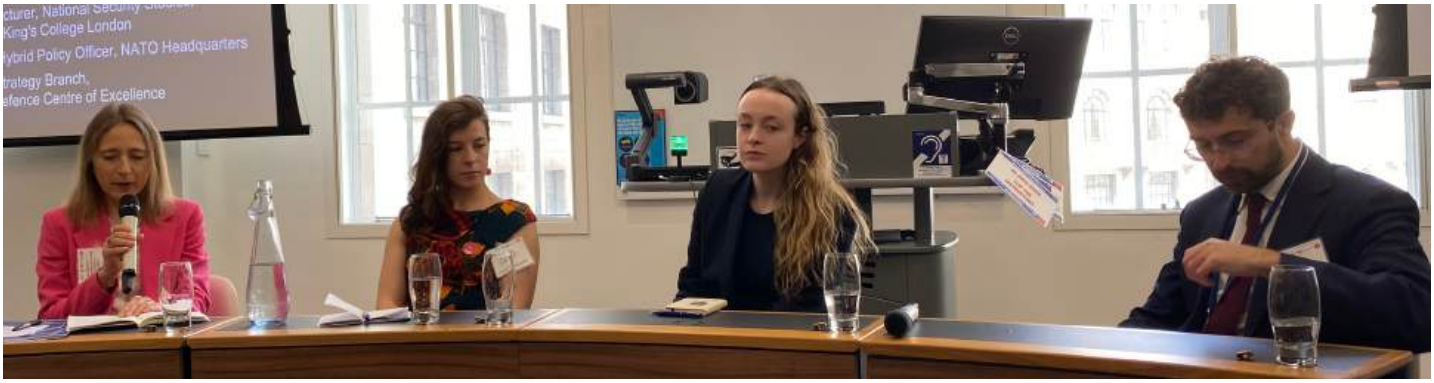
- Fiona Bradley, Cheffe de cabinet, Defence, Palantir Technologies
- Dr. Joe Devanny, Professeur associé, National Security Studies, Department of War Studies, King's College de Londres
- Dr. Amy Ertan, Responsable des politiques cyber et hybrides, Siège de l'OTAN
- Piret Pernik, Chercheuse, Division stratégie, Centre d'excellence de cyberdéfense coopérative de l'OTAN

Le panel plénier de l'atelier est parvenu à un consensus sur le fait que l'innovation technologique est une nécessité stratégique pour l'OTAN et qu'il faut prendre des risques pour conserver un avantage dans un monde de concurrence géopolitique accrue. Cependant, les processus d'approvisionnement de l'OTAN pour les technologies émergentes et de rupture sont largement considérés comme lents et mal adaptés au rythme d'innovation requis. Les programmes de l'OTAN comme le Plan d'action pour l'adoption rapide (PAAR), l'Accélérateur d'innovation de défense pour l'Atlantique Nord (DIANA) et le Fonds OTAN pour l'innovation (FNI) sont considérés comme des mécanismes prometteurs pour améliorer l'interopérabilité et rationaliser les délais d'approvisionnement, mais certains craignent que ces initiatives ne soient pas suffisamment efficaces. Tous les participants sont d'accord, les défis pour la cohésion de l'OTAN sont connus, mais la mise en œuvre de solutions à long terme reste difficile. Bien qu'il n'existe pas de panacée,



l'innovation et le développement de nouvelles technologies à double usage, en particulier celles liées à l'intelligence artificielle (IA), peuvent aider à combler les lacunes en matière de capacité. Cependant, la dépendance de la viabilité commerciale des technologies de défense émergentes vis-à-vis de la traction du marché civil a creusé le fossé de l'innovation entre les deux côtés de l'Atlantique. Les États membres reconnaissent que le budget consacré à l'innovation en matière de défense devrait augmenter, mais la question de savoir dans quelles capacités de défense se spécialiser et comment les rendre interopérables entre les membres de l'alliance demeure. Un développement excessif des capacités souveraines de l'IA, par exemple, pourrait nuire à l'interopérabilité de l'OTAN, tandis qu'une réglementation excessive et un manque de normalisation peut étouffer l'innovation, en particulier dans les systèmes numériques. Des collaborations « minilatérales » entre un petit groupe d'États, comme le partenariat AUKUS, ont été suggérées comme un terrain d'entente entre ces deux extrêmes.

L'OTAN subit un changement de priorité générationnel en matière de financement de ses capacités à mesure que de nouvelles technologies émergent rapidement. Il a été largement convenu de faciliter un environnement qui encourage l'innovation en matière de défense en incluant des partenaires de l'industrie et en créant des occasions d'expérimenter. Un tel environnement évite une dépendance excessive à l'égard de technologies, de capacités ou de partenaires industriels privés uniques et donne à tous les États membres une chance de participer à l'innovation. Bien que les mécanismes de l'OTAN comme DIANA et RAAP soient imparfaits, ils cherchent toujours à permettre des risques mesurés dans le financement de l'innovation en matière de défense. Le panel plénier a convenu qu'une innovation et une adoption rapides des technologies émergentes sont nécessaires, mais qu'il faudra trouver le juste équilibre entre l'amélioration des capacités et le maintien de la cohésion de l'alliance.



Groupe de discussion 1

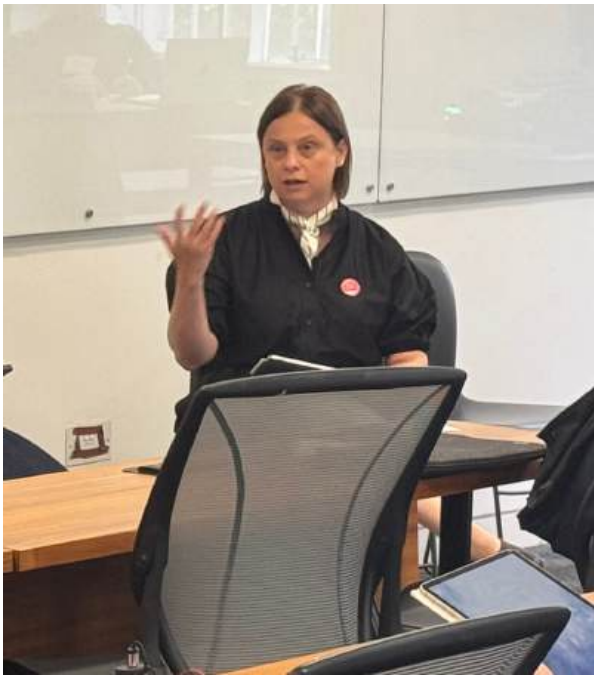
Visions concurrentes des EDT militaires

Groupe de discussion 1 : Visions concurrentes des EDT

- Professeur Antonio Calcara, Chargé de recherche principal, Centre for Security, Diplomacy and Strategy (CSDS), Vrije Universiteit Brussels
- Dr Raluca Csernatoni, Boursier, Carnegie Europe
- Dr Edward Hunter Christie, enseignant chercheur senior, Finnish Institute of International Affairs
- Dr Simona Soare, Maîtresse de conférences, Université de Lancaster

Remarques - Myrthe Bekkers, Étudiante, King's College de Londres

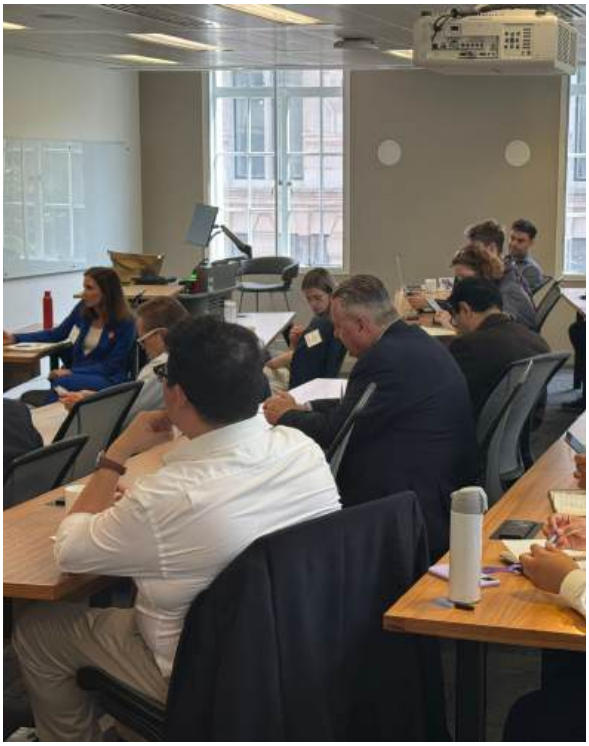
Les États membres de l'OTAN sont des pionniers des EDT militaires avancés dans toute une gamme de fonctions de combat interarmées, notamment le renseignement, la connaissance de la situation et le commandement et le contrôle. Alors que les principaux acteurs de l'OTAN investissent massivement dans des EDT à double usage de pointe, les alliés disposant de moins de ressources ont du mal à suivre le rythme. Comme ce groupe en a discuté, cette disparité pose des défis pour l'établissement d'une stratégie technologique cohérente. Le défi ne réside pas dans des priorités divergentes, mais dans la mise en œuvre d'objectifs communs dans les divers contextes nationaux de l'OTAN.



Visions et stratégies concurrentes

Comme point de départ de la conversation, le groupe a observé que les États membres s'accordent généralement sur l'importance des EDT pour la modernisation des forces armées. Les Alliés identifient des technologies clés similaires dans les documents d'orientation, conviennent de la nécessité de s'engager avec le secteur commercial et accordent la priorité à une approche « à l'échelle de la nation ». Dans le même temps, des différences notables subsistent, reflétant des priorités, des ambitions et une tolérance au risque nationales divergentes. Cette divergence est davantage compliquée du fait que les États-Unis accordent la priorité à la Chine en tant que défi sécuritaire, tandis que les alliés européens se concentrent sur la Russie. L'Europe s'est traditionnellement appuyée sur les États-Unis pour sa défense, mais la nécessité d'une plus grande autonomie européenne est de plus en plus reconnue, en particulier lorsque l'engagement des États-Unis s'affaiblit. Cependant, cette autonomie ne doit pas être absolue. Alors qu'une plus grande autonomie des États européens doit être l'objectif central, il convient de mettre un accent égal sur la cohésion de l'OTAN, la France étant mentionnée comme un exemple de membre qui équilibre ces priorités.

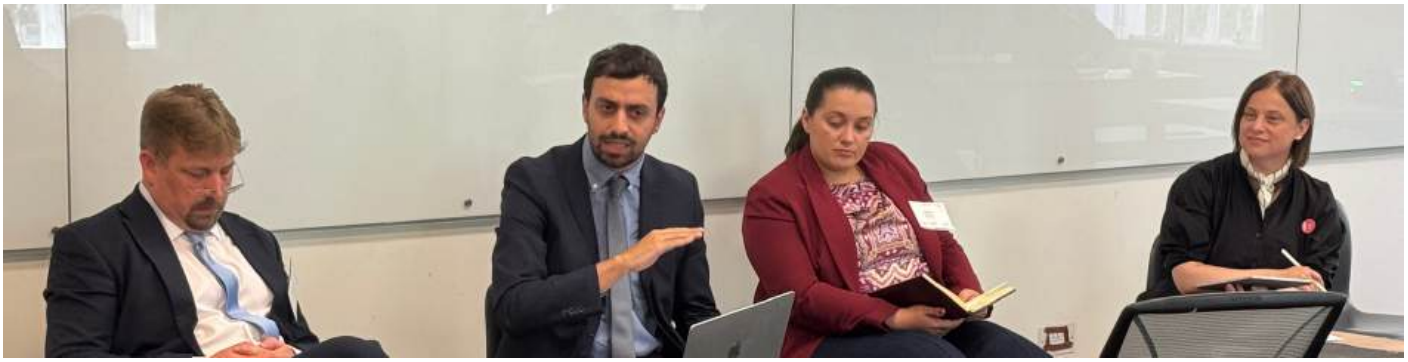
Interopérabilité



L'interopérabilité demeure un défi persistant au sein de l'OTAN, exacerbé par les disparités en matière d'investissement technologique, de capacités, de normes et d'accès aux technologies de pointe entre les États membres. La fragmentation de l'industrie européenne de la défense due à des budgets et priorités nationales différents entrave la modernisation cohérente et l'intégration des EDT. Comme souligné ci-dessus, des efforts comme DIANA et NIF visent à combler ces lacunes. Bien que l'efficacité de ces initiatives soit débattue, les participants ont noté que les deux montrent des succès certains et que leur mise en place au sein d'une organisation intergouvernementale de défense collective est en soi une réalisation importante.

Dynamique culturelle et facteur humain

Les panélistes ont souligné que les cultures de recherche et développement (R&D) militaires diffèrent considérablement entre les États-Unis et l'Europe. Les États-Unis sont considérés comme un innovateur de premier plan, tandis que les pays européens se perçoivent souvent comme des propulseurs ou des régulateurs technologiques. Un point crucial abordé par les participants était que les facteurs culturels et organisationnels, plutôt que les seuls achats ou financements, sont des obstacles majeurs à l'innovation en Europe. Bien que l'accès à des fonds suffisants soit essentiel à l'innovation, les participants ont souligné qu'il est au moins tout aussi important de disposer des bonnes personnes. La culture sociale et politique, y compris l'opinion publique et les attitudes générationnelles, jouent un rôle crucial dans la préparation et la mise en œuvre de l'innovation militaire. Favoriser les attitudes et les compétences qui contribuent à l'innovation nécessite un engagement civique, en particulier auprès des jeunes générations.



Innovation

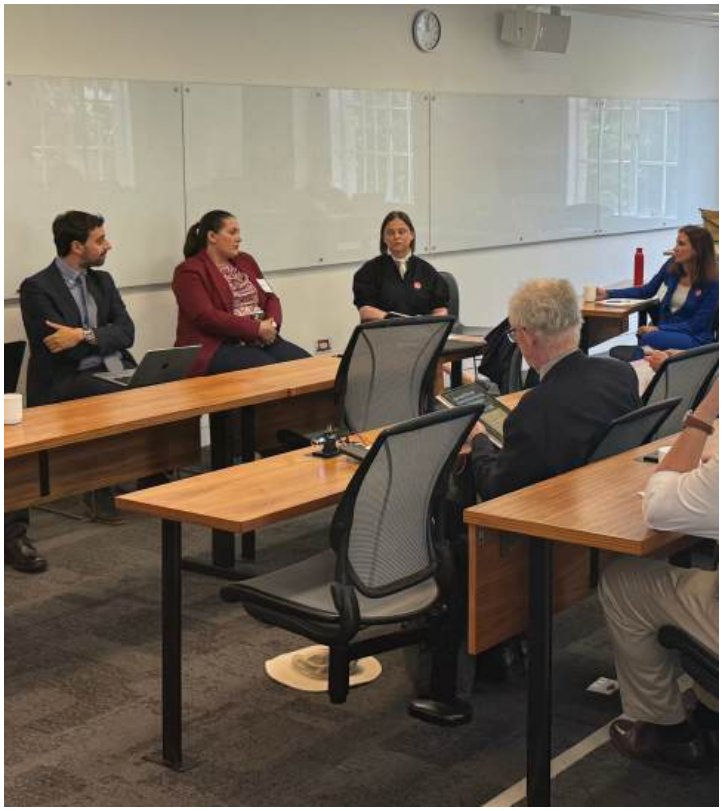
Pour favoriser davantage l'innovation, les processus d'approvisionnement doivent être plus adaptables et inclure les fournisseurs commerciaux, en particulier les experts en la matière (PME). Parallèlement, toutefois, un certain scepticisme subsiste quant au remplacement des grands groupes de défense traditionnels par une multitude de start-ups, l'intégration et la collaboration demeurant difficiles.

Il a plutôt été suggéré que l'intégration des technologies émergentes et de rupture (EDT) dans le secteur de la défense nécessite de nouvelles approches en matière de contractualisation et de collaboration entre les maîtres d'œuvre industriels et les entreprises de plus petite taille. Il est reconnu qu'il est nécessaire d'accélérer les modèles d'innovation ouverte qui engagent toutes les parties prenantes, partenaires commerciaux, universités et start-ups, plutôt que de s'appuyer uniquement sur des « innovations en pipeline » pilotées par le gouvernement.

Des innovations de pointe émergent dans des pays comme la France, les Pays-Bas, l'Allemagne, la Finlande et le Royaume-Uni, mais le déploiement à large échelle et la phase de transition restent des lacunes majeures. L'appétence pour le risque reste faible en ce qui concerne les achats et la planification demeure insuffisante pour l'intégration horizontale entre les nations. Le discours selon lequel « la réglementation entrave l'innovation » est contre-productif : une planification structurée de la transition vers l'innovation est essentielle. De plus, si les alliés de l'OTAN s'accordent largement sur les avantages stratégiques des EDT, leur impact variable et leur disponibilité pour une utilisation sur le champ de bataille nécessitent des approches nuancées et spécifiques au domaine pour leur intégration afin de garantir que une interopérabilité simple, plutôt que simplifiée par les nouvelles technologies, en particulier dans les environnements contestés.

Synergie UE-OTAN

Enfin, il a été souligné que la collaboration entre l'UE et l'OTAN s'améliore mais reste dépendante des gouvernements nationaux. Les structures sont naturellement complémentaires : les pouvoirs législatifs et budgétaires de l'UE offrent des possibilités de façonner les marchés de la défense, tandis que l'OTAN se concentre sur les normes et la coordination douce. La cohérence peut être assurée entre les 23 États membres des deux organisations. En particulier au niveau de l'UE, les discussions politiques évoluent et un leadership fort émerge de pays comme l'Allemagne. Cependant, les États membres de l'UE doivent démontrer leur engagement en fournissant le financement nécessaire.



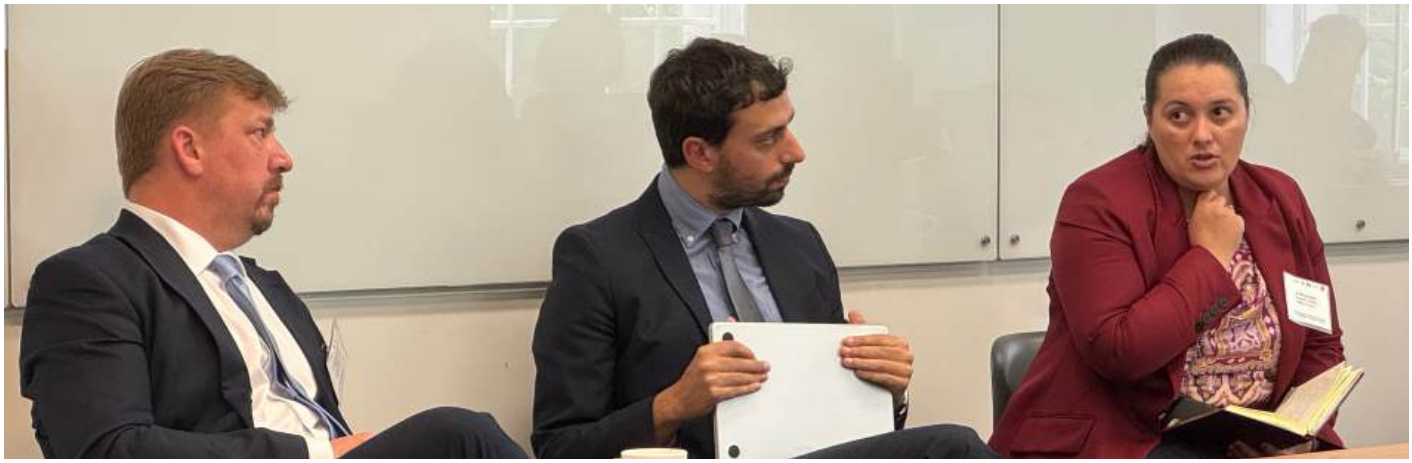
Les participants ont fait preuve d'un mélange d'optimisme et de pessimisme quant à la coopération et à la gouvernance future en matière d'EDT. Bien que des structures et des initiatives soient en place, des lacunes importantes subsistent dans la planification, l'exécution et l'adaptation culturelle. La question centrale n'est pas de savoir s'il faut investir dans les EDT, mais comment le faire efficacement, en veillant à ce que l'innovation soit planifiée, évolutive et intégrée dans l'ensemble de l'alliance. À terme, combler ces lacunes nécessitera un engagement soutenu et une vision commune pour transformer l'ambition en progrès opérationnel à un niveau global, au sein de l'OTAN.

Points à retenir :

- Les Alliés de l'OTAN partagent une vision unifiée de l'intégration des technologies de l'information et de la communication avancées, mais il reste d'importants défis à relever pour concrétiser cette ambition en raison des disparités en matière de ressources, de cultures d'innovation et d'interopérabilité.
- L'intégration des EDT dans l'ensemble de l'OTAN nécessitera un engagement soutenu, une planification et une exécution améliorées, un financement adéquat et une volonté de partager les risques.

Résultats : Identification et analyse des visions concurrentes de l'innovation technologique militaire entre les États-Unis et les pays membres de l'OTAN, en se concentrant sur les EDT

1. Les principaux membres de l'OTAN investissent massivement dans les technologies émergentes et de rupture (EDT), tandis que les alliés disposant de moins de ressources ont du mal à suivre le rythme.
2. Les attitudes culturelles à l'égard des risques et des perturbations varient : L'Europe penche vers l'optimisation et les changements progressifs, les États-Unis vers l'innovation audacieuse et la perturbation radicale.
3. Bien que des améliorations soient visibles, les dépenses et les priorités en matière de défense restent principalement décidées au niveau national. Il en résulte une fragmentation, en particulier dans l'UE, où les pays individuels poursuivent des ambitions distinctes, certains aspirant à l'autonomie technologique, d'autres acceptant des rôles de niche au sein de coalitions dirigées par les États-Unis.
4. Différents pays au sein de l'OTAN suivent des modèles de gouvernance différents pour la R&D militaire, les achats et la collaboration avec l'industrie, ce qui pourrait réduire la préparation technologique, l'interopérabilité et la cohésion à l'échelle de l'Alliance.
5. Les États-Unis perçoivent principalement la Chine comme leur principal défi de sécurité, moteur de leurs priorités technologiques ; la plupart des alliés européens se concentrent sur la Russie.
6. Les pays européens sont confrontés à des défis en matière d'augmentation rapide des investissements dans la défense. De plus, bien que les dépenses de défense de l'OTAN augmentent, certains États membres restent concentrés sur la préparation à court terme plutôt que sur les investissements technologiques à long terme.



Groupe de discussion 2

Domaines d'alignement de ces visions concurrentes

Groupe de discussion 2 : Domaines d'alignement de ces visions concurrentes

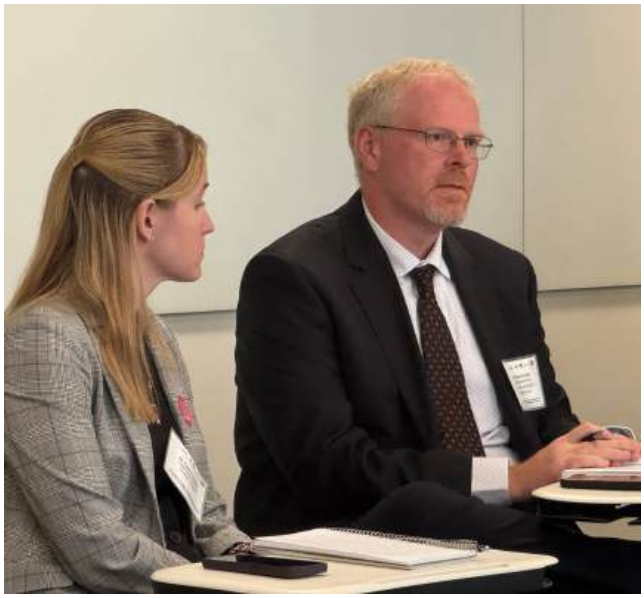
- KatyAnn Coulter, Responsable, Data Programs Branch ACC A29P, ACC/A29 Data Tech Futures Division, United States Air Force
- Benjamin Dunlap, Responsable de la branche des opérations de données, United States Air Force/Air Combat Command/A29
- Dr. Nathan Fisher, Responsable santé défense, Noblis, Inc.
- Dr. Kathryn H. Floyd, Directrice, Whole of Government Center of Excellence, William & Mary
- Huw Williams, Chercheur principal et rédacteur en chef, The Military Balance, International Institute for Strategic Studies

Remarques - Kyle Tucker, Étudiant, King's College de Londres et Université de St Andrews

Ce groupe a examiné les approches divergentes de l'innovation en matière de défense au sein de l'OTAN, en particulier entre les États-Unis et l'Europe. Les visions stratégiques et les priorités en matière de R-D pour la défense étaient largement harmonisées. Cependant, les méthodes par lesquelles les objectifs sont atteints varient considérablement. Le groupe a conclu que pour créer une collaboration plus étroite et des opérations conjointes plus efficaces, l'OTAN doit améliorer la normalisation des cadres de données et des technologies émergentes, soutenir l'expérimentation évolutive, tactique et locale, et démanteler les barrières institutionnelles qui empêchent une coordination efficace et le partage des connaissances au-delà des frontières.

Définition des visions et des priorités

Participants emphasised general conceptual alignment between European and U.S. approaches to defence innovation priorities. In particular, these priorities include the need to prepare for great-power conflict, leverage secure and agile AI systems, and empower tech-enabled decision-making. There is a decisive need to accelerate the scale and scope of current programmes, with a desire to innovate “on the edge”, something that European member states have fallen behind on compared to the U.S.

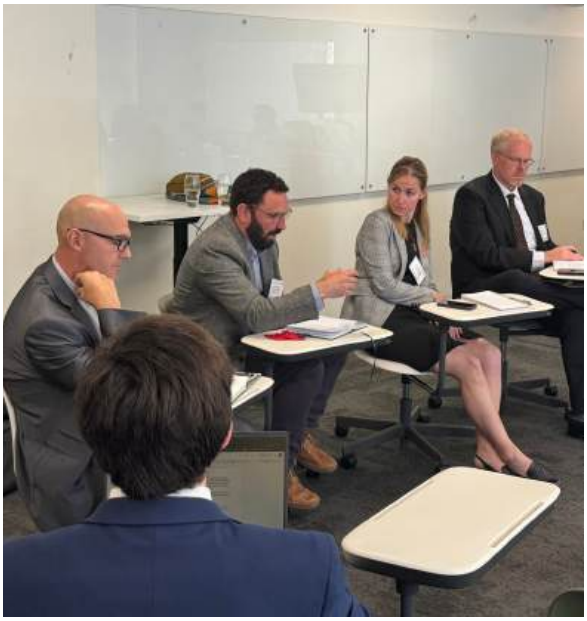


L'engagement en faveur de la collaboration et du partenariat est au cœur de tous les États membres. Cependant, il existe des différences culturelles entre les approches de l'innovation et de la sécurité nationale, les États-Unis se concentrant sur des développements plus pratiques tandis que l'Europe se concentre sur les aspects stratégiques et théoriques. L'intégration des deux approches au secteur par le biais d'un modèle de développement « accélérateur » visant à améliorer l'interopérabilité, la communication et la gestion des données a été identifiée comme une méthode permettant de concrétiser les visions et les priorités de l'OTAN.

Divergence de vision

Les participants ont franchement identifié les domaines dans lesquels les membres américains et européens de l'OTAN s'alignent mal, notamment en ce qui concerne l'appétence pour le risque, la rapidité de l'innovation et les cadres réglementaires. Les membres européens respectent des normes plus strictes en matière de protection des données et de confidentialité, ce qui limite l'intégration en temps réel des technologies émergentes. De plus, l'Europe met l'accent sur la dissuasion et la défense totale. Les États-Unis, en revanche, sont plus enclins à accepter le risque de vitesse et de préparation au combat. Alors que les partenaires américains et européens de l'OTAN sont préoccupés par le risque que la Russie représente pour l'alliance, la vision européenne est moins belliciste que celle des États-Unis vis-à-vis de la Chine en tant que défi stratégique.

Les cadres actuels de normalisation de l'OTAN restent optimisés pour les systèmes d'armes traditionnels à grande échelle et ne tiennent pas compte de la nature commerciale, à double usage et évolutive des technologies émergentes telles que l'IA et la biotechnologie. Les contrôles à l'exportation, en particulier la Réglementation américaine sur le trafic international d'armes (ITAR), ont été cités comme un goulot d'étranglement pour le partage des données. Les réglementations européennes sur le capital-risque, ainsi que le manque de start-ups privées de capital-risque et de défense travaillant avec des technologies à double usage, limitent également la capacité d'innovation européenne en matière de défense. Sans un moyen standardisé de traiter les données classifiées à travers l'alliance, l'innovation est limitée. L'augmentation de la normalisation peut accélérer la vitesse du cycle d'approvisionnement.



Domaines de convergence ou d'alignement

Pour améliorer l'interopérabilité et la collaboration, les participants ont appelé à l'élaboration de normes consensuelles concernant la gestion des données et les technologies à double usage, en particulier lorsque les cycles de développement commercial dépassent l'adaptation des politiques. Les normes devraient permettre des tests rapides et la diffusion des résultats. Tous s'accordent sur le rôle de l'industrie privée, mais l'harmonisation des approches américaine et européenne sera cruciale pour renforcer la capacité d'accélérer le cycle de R&D et d'innovation.

En termes de processus, alors que le partage des données et des meilleures pratiques devrait être centralisé, l'expérimentation et les tests devraient être délégués au niveau tactique et au niveau de l'État, faisant écho à la discussion sur les relations « minilatérales » lors du panel plénier. De plus, il est crucial d'avoir une plus grande tolérance à l'échec dans le processus d'innovation. La promotion des leçons reproductibles tirées de la guerre russo-ukrainienne et la possibilité d'approches ascendantes pour la spécialisation ont également été notées. Par exemple, l'Estonie a dirigé le Centre d'excellence coopératif de cyberdéfense de l'OTAN en raison de la vitalité de sa communauté de cybersécurité locale et du soutien actif du gouvernement estonien.

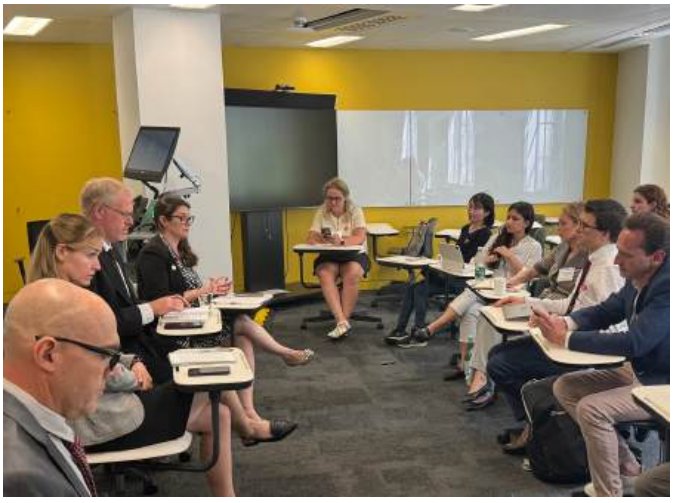
En termes de processus, alors que le partage des données et des meilleures pratiques devrait être centralisé, l'expérimentation et les tests devraient être délégués au niveau tactique et au niveau de l'État, faisant écho à la discussion sur les relations « minilatérales » lors du panel plénier. De plus, il est crucial d'avoir une plus grande tolérance à l'échec dans le processus d'innovation. La promotion des leçons reproductibles tirées de la guerre russo-ukrainienne et la possibilité d'approches ascendantes pour la spécialisation ont également été notées. Par exemple, l'Estonie a dirigé le Centre d'excellence coopératif de cyberdéfense de l'OTAN en raison de la vitalité de sa communauté de cybersécurité locale et du soutien actif du gouvernement estonien.

Points à retenir:

- Moderniser les cadres de normalisation de l'OTAN pour soutenir l'interopérabilité et l'adoption des EDT.
- Réformer les barrières réglementaires et institutionnelles au niveau des États et des alliances pour permettre une innovation plus rapide.
- Développer l'innovation ascendante et les chaînes d'approvisionnement grâce à des partenariats minilatéraux, à des expérimentations localisées et à des investissements dans le capital humain.

Résultats : Identification des domaines dans lesquels les approches des États-Unis et de l'OTAN en matière de R&D militaire peuvent être alignées pour favoriser une collaboration plus étroite et des opérations conjointes plus efficaces.

1. Standardisation de l'infrastructure numérique et de la gestion des données.
2. Cadres partagés pour le développement, l'intégration et la gestion des EDT.
3. Harmonisation des différences de tolérance au risque, de perception de la menace et de culture de l'innovation.
4. Des modèles d'approvisionnement flexibles qui permettent une expérimentation localisée et une spécialisation nationale volontaire.



5. Amélioration de la coordination de la logistique, des chaînes d'approvisionnement et des cycles de R&D militaire.

Groupe de discussion 3

Renseignements sur les cybermenaces (CTI) Partage entre alliés de l'OTAN

Groupe de discussion 3 : Partage de renseignements sur les cybermenaces (CTI) entre les alliés de l'OTAN

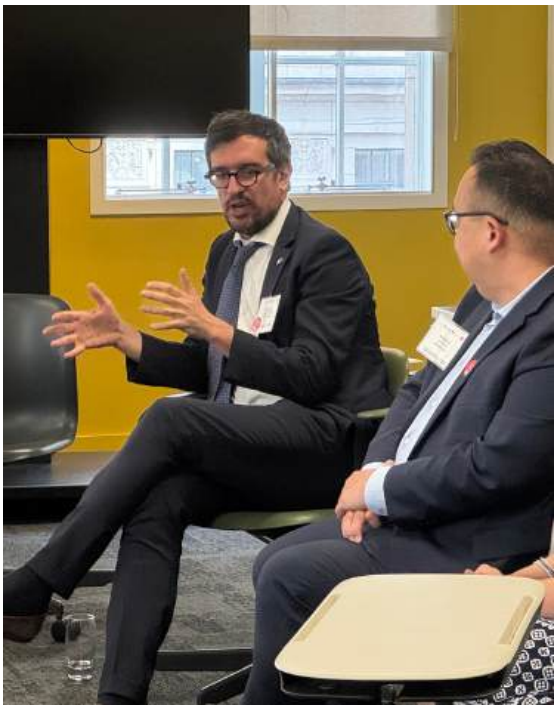
- Eman Blair, Vice-président exécutif pour le développement technologique et conseiller spécial, Pentagon Federal Credit Union
- Sally Daultrey, Associée, Whole of Government Center of Excellence, William & Mary
- Dr. Andrea Gilli, Maître de conférences, Université de St Andrews
- Roger Yee, Associé principal, Outcome One

Remarques - Alex Bumpers, Étudiant, King's College de Londres

Pour maintenir la sécurité dans l'environnement actuel des menaces multidomaines, l'OTAN et ses alliés ont besoin de solides capacités de cyberdéfense, y compris un partage efficace des renseignements sur les cybermenaces (CTI) pour détecter, prévenir et réagir aux cyberactivités malveillantes. Bien qu'un ensemble de mécanismes de cyberdéfense de l'OTAN existe actuellement et présente des caractéristiques communes entre alliés, plusieurs défis — dont certains ne sont pas uniquement techniques — compromettent l'efficacité du partage de renseignements sur les cybermenaces (CTI) entre les États membres et leurs alliés. Pour relever ces défis, ce panel a recherché des perspectives intersectorielles sur les meilleures pratiques pour améliorer le partage de CTI, y compris des idées sur la façon dont les technologies émergentes comme l'IA pourraient améliorer l'échange de données en temps réel et les stratégies de défense collaboratives.

Asymétrie et renseignement sur les cybermenaces

L'asymétrie des capacités, des ressources et des chaînes d'approvisionnement entre les membres de l'OTAN et les alliés remet en question la rapidité avec laquelle un partage efficace des CTI peut être réalisé. Le groupe a convenu que les cyberexercices conjoints peuvent être utiles pour identifier et combler les lacunes en matière de capacités et de responsabilisation. Grâce à des simulations de crise des stratégies de coopération en matière de cyberdéfense existantes ou prévues, les parties prenantes peuvent identifier les avantages comparatifs et déléguer des rôles et des responsabilités clairs qui jouent sur les forces de chaque membre et partenaire de l'OTAN.



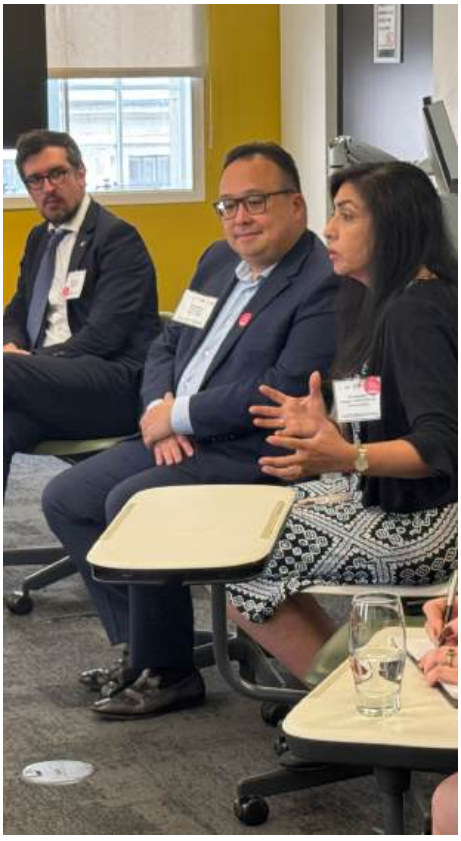
L'IA offre à la fois des avantages potentiels et des risques pour un partage efficace des CTI. Des modèles d'IA formés à la connaissance de la cybersécurité et de la détection des cybermenaces pourraient accélérer la formation des membres de l'OTAN ayant moins d'expertise, en fournissant une base de connaissances crédible pour l'apprentissage et le développement.

Cependant, des taux divergents de développement et d'adoption de l'IA peuvent présenter de nouvelles formes d'asymétrie et des risques potentiels pour la sécurité, tels que des modèles « empoisonnés » par des données corrompues. À mesure que de plus en plus de pays développent leurs propres modèles, ils peuvent hésiter à partager leurs capacités en raison de la classification, des problèmes de sécurité ou de la concurrence.

Rôles et responsabilités dans tous les secteurs

Les participants se sont mis d'accord sur le caractère impératif des partenariats public-privé pour un partage efficace des CTI et pour gérer l'innovation dans les technologies émergentes afin de stimuler la cyberdéfense de l'OTAN. Les entreprises privées de CTI ont une visibilité mondiale sur le paysage des cybermenaces, au-delà de celle des gouvernements les plus compétents. Le groupe a discuté de la manière dont les acteurs privés pourraient être mieux placés pour coordonner le partage de CTI en raison de leur visibilité plus large et de leur capacité à utiliser des réseaux informels pour la communication et l'alerte, en particulier pour les menaces plus urgentes.

Le groupe a discuté de la façon dont des incitations divergentes - œuvrer pour le bien public ou pour le profit - peuvent saper des partenariats efficaces entre les secteurs public et privé. Les acteurs privés en particulier peuvent être réticents à partager des informations sur les cybermenaces ou des outils qui, selon eux, leur confèrent un avantage concurrentiel sur le marché. Un partage et une délégation efficaces des rôles et des responsabilités en matière de CTI nécessitent des solutions créatives qui équilibrent les avantages comparatifs et les incitations distincts de chaque secteur.



Menaces et nature du cyberespace

Les participants ont examiné comment la nature virtuelle et transfrontalière du cyberespace complique la perception des menaces et compromet l'urgence. Des menaces telles que des actes de terrorisme entraînant des blessures physiques peuvent susciter une plus grande urgence et une plus grande volonté de coopérer en matière de partage de renseignements. Le groupe a discuté de la manière dont les États-Unis respectent un mandat d'« obligation d'avertir » qui les oblige à alerter les autorités compétentes de tout pays en cas de menace connue contre la vie. Le mandat a conduit les États-Unis à alerter la Russie avant une attaque terroriste à Moscou en 2024, montrant une capacité de coopération même entre adversaires. Cependant, le fait que les cybermenaces présentent rarement des blessures, et encore moins des menaces pour la vie, complique l'application des structures de responsabilisation et d'incitation existantes comme l'« obligation d'avertir ».

Confiance

Le groupe a exploré les différences entre la confiance émergente qui croît lentement avec le temps et la confiance qui apparaît en cas d'urgence. Les deux formes sont essentielles pour un partage efficace de CTI, mais peuvent être minées par des objectifs concurrents, même entre alliés et partenaires.

Par exemple, les États-Unis ont temporairement suspendu le partage de renseignements avec l'Ukraine au milieu des tensions diplomatiques au début de 2025. Les membres et partenaires de l'OTAN peuvent ne pas faire confiance à la sécurité des infrastructures critiques ou des systèmes de cyberdéfense des alliés ; beaucoup accordent la priorité à l'adoption de technologies fabriquées dans le pays. Le groupe a convenu que la compréhension de la tolérance au risque est un élément nécessaire du partage de CTI, et que la position traditionnelle d'aversion au risque des gouvernements doit se transformer pour faciliter un partage efficace de CTI.

Le facteur humain

Le partage de CTI est souvent discuté en termes purement techniques, tandis que les facteurs humains qui conduisent à un partage réussi sont négligés. L'accent mis sur les barrières technologiques néglige les défis humains liés à la confiance et à la culture organisationnelle qui peuvent bloquer ou permettre le partage. Les participants ont discuté de la façon dont diverses définitions des CTI ont émergé et ont convenu que le partage efficace repose sur un consensus entre les parties impliquées sur ce qui est partagé, avec qui et selon quelles attentes. L'intelligence s'inscrit toujours dans un contexte ; alors que l'IA peut automatiser les processus pour aider à signaler les cyberactivités malveillantes, un partage de CTI efficace sera alimenté par l'intuition, l'intelligence et l'action humaines.

Points à retenir :

- Mener des cyberexercices et des hackathons conjoints pour clarifier les rôles et les responsabilités en matière de partage de CTI entre les membres et les partenaires de l'OTAN, renforcer les stratégies de défense collaboratives et identifier les scénarios susceptibles de mettre à rude épreuve la confiance pour permettre une atténuation proactive.
- Rationaliser les partenariats public-privé pour le partage de CTI en développant des solutions qui alignent les incitations divergentes entre les deux secteurs pour éviter les tensions qui peuvent saper la confiance et la coopération.
- Tirer parti de l'IA pour automatiser les processus d'indicateurs et d'alertes et soutenir la formation des parties prenantes les moins cybernétiques tout en atténuant l'asymétrie et les risques de sécurité supplémentaires liés à l'IA qui pourraient saper la confiance et l'interopérabilité.

Résultats : Identification des meilleures pratiques pour améliorer le partage de renseignements sur les cybermenaces avec l'OTAN, en tirant parti de l'IA pour améliorer l'échange de données en temps réel et les stratégies de défense collaboratives.

- Fournir des renseignements sans dicter comment ils doivent être utilisés.

- Travailler à partir d'une compréhension partagée de la mission et des menaces crée une culture de collaboration et de volonté de contribuer au renseignement.
- Travailler à partir d'une définition partagée des renseignements sur les cybermenaces entre les partenaires.
- Identifier les lacunes dans les processus de partage de CTI grâce à des cyberexercices conjoints et des hackathons.
- La plateforme OTAN de partage d'informations sur les logiciels malveillants et le système CVE (Common Vulnerabilities and Exposures) sont très efficaces.
- En commençant par de petites étapes et en s'orientant vers des processus plus robustes pour le partage de CTI.
- Partager les faiblesses connues de la cyberdéfense, telles que des techniques de stockage inappropriées, par opposition aux seules informations relatives aux menaces urgentes.
- Veiller à ce que les perspectives des praticiens soient représentées dans les discussions sur la manière d'améliorer le partage de CTI.
- Utiliser des réseaux informels pour le partage de CTI, en particulier pour les menaces plus urgentes où une communication rapide est essentielle, lorsque cela est possible.
- Utiliser des normes de données partagées entre les partenaires.