ASSEMBLEE PARLEMENTAIRE DE L'OTAN

COMPTE RENDU

DE LA RÉUNION DE LA

COMMISSION DES SCIENCES ET DES TECHNOLOGIES

Samedi 1er juin 2019

Music Hall
Château de Bratislava
Bratislava, Slovaquie

128 STC 19 F | Original : anglais | 13 juin 2019

LISTE DE PRÉSENCE

Présidente de la commission	Maria MARTENS (Pays-Bas)
Rapporteure générale	Susan DAVIS (États-Unis)
Rapporteur	Matej TONIN (Slovénie)
Présidente de l'AP-OTAN	Madeleine MOON (Royaume-Uni)
Secrétaire général de l'AP-OTAN	David HOBBS

Délégations membres

Belgique	Brigitte GROUWELS
	Damien THIERY
Canada	Joseph A. DAY
Croatie	Nenad STAZIC
	Miroslav TUDJMAN
Espagne	Begona NASARRE
France	Anissa KHEDHER
	Joachim SON-FORGET
Hongrie	Agnes VADAI
Islande	Arna Gerdur BANG
	Njall Trausti FRIDBERTSSON
Italie	Andrea CANGINI
	Fabrizio ORTIS
Lettonie	Aldis BLUMBERGS
Lituanie	Vytautas BAKAS
	Dainius GAIZAUSKAS
	Rasa JUKNEVICIENE
Luxembourg	Sven CLEMENT
	Roberto TRAVERSINI
Monténégro	Obrad Miso STANISIC
Pays-Bas	Sven KOOPMANS
	Janny VLIETSTRA
Norvège	Lene WESTGAARDE-HALLE
Pologne	Jozef LYCZAK
Portugal	Bruno VITORINO
Slovaquie	Milan KRAJNIAK
	Juraj SOBONA
Suède	Karin ENSTROM
Turquie	Hisyar OZSOY
	Kamil SINDIR
	Taner YILDIZ
Royaume-Uni	Baroness ADAMS
	Douglas CHAPMAN
	Kevan JONES
	Baroness RAMSAY OF CARTVALE
	Andrew ROSINDELL
États-Unis	Neal DUNN
	James SENSENBRENNER
	John SHIMKUS

Délégations associées

Arménie	Gevorg GORGISYAN
Azerbaïdjan	Malahat IBRAHIMGIZI
Bosnie-Herzégovine	Nikola LOVRINOVIC
Finlande	Tom PACKALEN
	Mikko SAVOLA
Macédoine du Nord	Katerina KUZMANOVSKA
Suisse	Pierre-Alain FRIDEZ

Délégations partenaires régionaux et membres associés méditerranéens

Maroc	Mohammed AZRI

Intervenants

Lukas PARIZEK
Secrétaire d'État, ministère des affaires étrangères et européennes, République slovaque

Jan-Peter KLEINHANS
Directeur de projet sécurité IdO, *Stiftung Neue Verantwortung* (SNV)

Helena LEGARDA
Chercheuse associée, Institut Mercator sur la Chine (MERICS)

Pavel ZUNA
Directeur, Bureau de soutien à la collaboration de l'Organisation OTAN pour la science et la technologie (OTAN STO CSO)

Secrétariat international

Henrik BLIDDAL, directeur
Ginevra SPONZILLI, coordinatrice
Gillian HANNAHS, assistante de recherche
Angelica PUNTEL, assistante de recherche

I. Remarques préliminaires de Maria MARTENS (Pays-Bas), présidente

1. La présidente de la commission des sciences et des technologies (STC), **Maria Martens** (NL), déclare ouverte la réunion de la commission des sciences et des technologies de la session de printemps 2019. Elle souhaite la bienvenue à tous les membres et remercie la délégation slovaque pour l'organisation de cette session.

2. Elle fournit des informations pratiques sur la participation à la réunion, le passage aux sessions sans support papier, la biographie des intervenants, les réseaux sociaux et l'ordre du jour.

II. Adoption du projet d'ordre du jour [086 STC 19 F]

3. **Le projet d'ordre du jour [086 STC 19 F] est adopté.**

III. Adoption du compte rendu de la réunion de la commission des sciences et des technologies tenue à Halifax, Canada, le dimanche 18 novembre 2018 [249 STC 18 F]

4. **Le compte rendu [249 STC 18 F] est adopté.**

IV. Examen des *Commentaires du secrétaire général de l'OTAN, président du Conseil de l'Atlantique Nord, sur les recommandations de politique générale adoptées en 2018 par l'Assemblée parlementaire de l'OTAN* [043 SESP 19 F].

5. La présidente prend acte des *Commentaires du secrétaire général de l'OTAN, président du Conseil de l'Atlantique Nord, sur les recommandations de politique générale adoptées en 2018 par l'Assemblée parlementaire de l'OTAN* [043 SESP 19 F].

6. Les membres de la commission ne formulent aucun commentaire.

V. Exposé par Lukas PARIZEK, secrétaire d'État, ministère des affaires étrangères et européennes sur *Le futur des mesures de confiance et de sécurité et de la maîtrise des armements dans le cadre de l'OSCE : perspective de la présidence slovaque de l'OSCE.*

7. Le secrétaire d'État, **Lukas Parizek,** commence son intervention en soulignant que l'Organisation pour la sécurité et la coopération en Europe (OSCE) et l'OTAN sont les piliers de l'architecture de sécurité euro-atlantique. Ces deux institutions ont été créées pour garantir la sécurité des citoyens dans l'espace euro-atlantique. Elles ont permis d'en faire un espace sécurisé, sûr et stable pour ses citoyens. En 2019, la présidence slovaque de l'OSCE a fixé trois priorités : Premièrement, elle souhaite que l'OSCE mette encore davantage l'accent sur la prévention et la résolution des conflits. Deuxièmement, qu'elle veille à la sécurité future des populations dans la région de l'OSCE et au-delà avec un accent sur la coopération et les menaces hybrides. Troisièmement, la Slovaquie voudrait se concentrer sur un multilatéralisme efficace, dans la mesure où il est indispensable que la sécurité repose sur une coopération globale et inclusive.

8. Dans le cadre de la dimension militaire de l'OSCE, l'organisation soutient la mise en œuvre de mesures de prévention des conflits. M. Parizek souligne que l'OTAN et l'OSCE devraient travailler de concert pour mettre à jour ces mesures et établir un suivi de la mise en

œuvre. Dans ce sens, il est fondamental de rétablir la confiance entre les acteurs internationaux. La Slovaquie a soutenu les dialogues structurés qu'elle considérait comme des forums essentiels pour veiller à maintenir, dans la continuité, des relations de confiance entre les États.

9. Il souligne que le monde n'a jamais été véritablement sûr : à l'heure actuelle, les déséquilibres dans la distribution des richesses, l'arrogance, l'ignorance et l'exclusion sociale sont autant d'éléments qui ont contribué à faire monter l'extrémisme. Par conséquent, on ne devrait pas uniquement mettre l'accent sur les menaces militaires. Les synergies entre l'OSCE et l'OTAN devraient être développées pour faire face à ces nouveaux défis. La coordination et le partage d'informations devraient également faire partie des priorités.

10. La présidente ouvre la discussion en demandant quel est le statut des relations entre l'OSCE et la Russie. D'autres questions portent sur des idées concrètes de coopération renforcée entre l'OSCE et l'OTAN ainsi que sur les efforts de l'OSCE dans les domaines tels que la cybersécurité, les réseaux sociaux, les opérations d'information, les discours haineux et les flux de migration.

11. M. Parizek souligne que l'OSCE est une plateforme de discussion efficace avec la Russie, étant donné que chaque État participant de l'OSCE a la même voix et le même droit de véto. Il concède que les évènements de 2014 et la crise actuelle en Ukraine avaient eu un impact sur le fonctionnement de l'organisation, mais que le débat reste une valeur centrale de l'organisation. En outre, à l'est de l'Europe, l'OSCE reste très populaire et connue et les pays de la région reconnaissent largement la valeur de sa mission. La Russie fait partie de l'OSCE et toute menace à la sécurité doit être discutée dans le cadre de l'organisation.

12. Il indique que la coopération avec l'OTAN date des années 1990. Actuellement, l'OTAN apporte une protection et un soutien logistique aux missions de l'OSCE. Par exemple, le processus d'observation des élections en Afghanistan s'est fait en coopération avec l'OTAN. Il déclare que les deux organisations devraient toujours trouver de nouvelles façons de travailler ensemble et de se soutenir mutuellement pour améliorer leur efficacité. Concernant la migration, M. Parizek explique que les différentes présidences ont fait de cet objectif leur priorité, y compris la présidence slovaque actuelle. Cette question a été principalement abordée à travers le dialogue avec les pays méditerranéens partenaires.

13. L'intervenant note que le concept de sécurité s'est élargi. La cybersécurité, ajoute-t-il, est un nouvel axe du travail de l'OSCE en matière de sécurité. Il concède que l'organisation y est arrivée un peu tard. Un collègue de M. Parizek au ministère des affaires étrangères, l'ambassadeur **Robert Kirnag,** décrit les efforts menés actuellement par l'OSCE dans le domaine de la cybersécurité. L'organisation s'est principalement concentrée sur la cybersécurité des États, et non sur la cybercriminalité en tant que telle, par exemple. Les efforts de cybersécurité se sont articulés autour des mesures visant à rétablir la confiance, de la coopération régionale et de la protection des infrastructures critiques. En ce qui concerne les discours haineux, il souligne l'importance d'instruments tels que les séminaires éducatifs de l'OSCE. Selon lui, ils doivent être conjugués à un travail sur la tolérance et la non-discrimination.

VI. Exposé par Pavel ZUNA, directeur, Bureau de soutien à la collaboration de l'Organisation OTAN pour la science et la technologie (OTAN STO CSO), Paris, sur *Le programme de travail collaboratif de l'OTAN (CPoW) : conserver l'avance scientifique et technologique*, suivi d'un débat

14. **Pavel Zuna** commence sa présentation en se référant aux différents objectifs établis en 2019 dans le cadre des directives politiques de l'OTAN qui ont trait aux sciences et technologies (S&T) :
- maintenir l'avantage technologique de l'Alliance ;
- accélérer le développement capacitaire ;
- rester à la pointe de la S&T ;
- augmenter les démonstrations de prototypes ; et
- permettre une transition rapide des technologies.

15. M. Zuna rappelle que le principal objectif de l'Organisation pour la science et la technologie (STO) est de maintenir l'avantage technologique et de renforcer la souplesse de l'Alliance. La STO emploie différents modèles pour atteindre cet objectif :

- un modèle collaboratif qui fournit aux membres de l'OTAN un forum permettant d'employer des ressources pour définir, mener, et promouvoir la recherche en matière de coopération et l'échange d'informations ; et
- un modèle interne au sein du centre de recherche marine et d'expérimentation (CMRE), où les activités sont menées dans un laboratoire exécutif dédié doté de personnel, de capacités et d'infrastructures.

16. Au CSO, le cœur du modèle collaboratif comprend différents panels et groupes qui gèrent une grande variété d'activités de recherche scientifique et qui soutiennent les besoins de gestion de l'information de l'organisation. Il ajoute que ces panels sont constitués de scientifiques de renommée internationale, d'ingénieurs et de spécialistes de l'information. En plus d'apporter une supervision technique cruciale, ces panels offrent également un lien de communication entre les utilisateurs militaires et d'autres organes de l'OTAN. Actuellement, le programme de travail collaboratif (CPoW) de l'OTAN réunit quelque 6 000 scientifiques, ingénieurs et analystes qui travaillent sur plus de 300 activités de recherche par an. Les pays les plus actifs sont ceux qui disposent d'une solide infrastructure de recherche et d'industrie, tels que le Canada, la France, l'Allemagne, les Pays-Bas, le Royaume-Uni, et les États-Unis.

17. M. Zuna annonce aux membres de la commission que le budget de son bureau est d'environ 6,6 millions d'euros. Si l'on ajoute à ce chiffre celui des ressources nationales allouées au CPoW, plus de 500 millions d'euros ont été dépensés annuellement pour les S&T à l'OTAN. Il ajoute que le programme avait soutenu les États dans la mise en place de leurs capacités nationales et aidé l'OTAN à établir ses propres capacités. Il indique qu'il existe une bonne collaboration entre le Commandement allié transformation (ACT) et le Groupe consultatif industriel OTAN (NIAG).

18. Il décrit ensuite les faits marquants du CPoW, notamment en matière de mobilité militaire ; méga données ; systèmes maritimes sans pilote ; capacité alliée de surveillance future ; accélération du développement des capacités et de l'exécution ; partenariats structurés avec l'ACT, le Commandement allié opérations et le NIAG. Enfin, il mentionne le rapport de la STO *Tech Trends Report 2018*, qui décrit les conséquences des nouvelles technologies à court, moyen et long termes.

19. Le débat qui suit permet d'aborder de nombreuses questions sur la recherche relative à :
– la navigation satellite dans le Grand Nord ;
– les véhicules aériens sans pilote (UAV), y compris les dispositifs permettant de les contrer ;

– les questions juridiques, éthiques et morales relatives aux systèmes d'armement létaux autonomes ;
– les armes hypersoniques ;
– l'importance des réseaux sociaux dans un contexte opérationnel ;
– les ressources financières de l'Organisation OTAN pour la science et la technologie ; et
– l'usage de l'intelligence artificielle (IA) dans les prises de décision.

20. M. Zuna commence en déclarant que les scientifiques et les ingénieurs devraient voir plus loin que les capacités actuelles de navigation par satellite. Par exemple, il signale que l'évolution des sciences quantiques pourrait permettre de développer des systèmes de navigation plus précis. Il prévient que la Chine pourrait devancer l'Alliance dans ce domaine. Il poursuit en indiquant que la détection et l'identification sont les premières mesures indispensables dans le domaine de la défense contre les UAV. Il signale aux délégués que les chercheurs examinent différents systèmes de radars permettant la détection des UAV. Il souligne que l'OTAN est en train de développer des politiques relatives aux aspects juridiques, éthiques et moraux concernant les UAV. En parallèle, les scientifiques travaillent sur de nouvelles technologies permettant à l'Alliance de maintenir un contrôle probant des systèmes basés sur l'intelligence artificielle. Au sujet des armes hypersoniques, il déclare que certaines limites physiques n'ont pu être dépassées ni par l'OTAN ni par la Russie, même si cette dernière prétend souvent le contraire. Par exemple, certains missiles hypersoniques ont opéré à des vitesses et dans une couche de l'atmosphère qui ont rendu les communications impossibles. Concernant les réseaux sociaux dans un contexte opérationnel, M. Zuna fait part des efforts de la S&T de l'OTAN visant à comprendre les mécanismes de guerre hybride dans la région du Donbass, sur demande de l'Ukraine. À propos de l'emploi du budget du STO, il déclare que son bureau soutient peu les activités et la coopération entre les États membres et ne finance aucun effort de recherche. Il conclut en faisant état d'une initiative ayant pour but d'analyser le potentiel de l'intelligence artificielle dans l'appui à la prise de décisions.

VII. Examen du projet de rapport général *L'OTAN et le cyberespace : renforcer la sécurité et la défense, stabiliser la dissuasion* [087 STC 19 F], présenté par Susan DAVIS (États-Unis), rapporteure générale

21. **Susan Davis** (US) entame la présentation de son projet de rapport général en soulignant que la société d'aujourd'hui est de plus en plus interconnectée et que les cybermenaces enregistrent une hausse spectaculaire. Les réseaux appartenant à l'OTAN ont subi tous les mois des centaines de cyberincidents, sans parler des intrusions sur les réseaux critiques des Alliés, qui augmentent considérablement. Son projet de rapport porte sur les menaces à la cybersécurité qui sont au cœur de la raison d'être de l'OTAN comme des cyberattaques qui menaceraient l'intégrité territoriale, l'indépendance politique ou la sécurité nationale des États membres de l'OTAN, par exemple les cyberattaques et qui pourraient mener un Allié à invoquer l'article 5.

22. Mme souligne que la cybersécurité, la défense et la dissuasion sont devenues des tâches essentielles de l'OTAN. Par conséquent, une cyberattaque suffisamment néfaste contre un Allié pourrait être considérée comme une attaque armée contre l'ensemble de l'Alliance. En 2018, les Alliés avaient réaffirmé leur volonté d'employer toutes leurs capacités pour lutter contre les menaces dans le cyberespace, dont ils avaient fait un domaine d'opérations à part entière. Elle rappelle que les Alliés ont pris des mesures significatives pour intégrer aux opérations leurs capacités dans le cyberespace. Outre la cybersécurité, la défense et la dissuasion, elle indique que les normes internationales pourraient également être utilement intégrées aux stratégies de cybersécurité des Alliés. Elle énumère également les actions concrètes de l'OTAN dans ce domaine, telles que la création d'un centre d'opérations dans le cyberespace, de plusieurs projets de cyberdéfense intelligente, le cyberpartenariat de l'OTAN avec l'industrie et la coopération cruciale avec l'Union européenne.

23. Elle fait ensuite le point sur la façon dont les États tentent de prévenir les cyberattaques. L'aptitude à signaler ses capacités de représailles et sa détermination est fondamentale. Étant donné qu'il est difficile de faire passer un message dans le cyberespace, elle rappelle la doctrine américaine de l'« Engagement durable » : les Alliés pourraient développer un avantage stratégique en maintenant un niveau d'action continu à travers l'utilisation de leurs cybercapacités. Elle a également posé la question de savoir si, dans la mesure où la cyberdéfense est une compétence nationale, il était du ressort de l'OTAN d'élaborer des stratégies de dissuasion collective et des politiques de sécurité. Et, le cas échéant, quelle forme pourraient prendre ces stratégies et politiques ?

24. Les questions et déclarations des délégués portent sur plusieurs éléments fondamentaux :

- comment déterminer qui est à l'origine des cyberopérations et est-ce que les États devraient attribuer publiquement ces opérations à des acteurs étatiques ;
- comment partager les informations entre Alliés ;
- l'OTAN doit-elle se saisir des questions liées au cyberespace ;
- si l'article 5 était invoqué, quelle serait la bonne réponse à apporter ;
- comment améliorer la coopération entre l'OTAN et les équipes nationales d'intervention en cas de crise informatique ;
- quand et comment les entreprises et l'État devraient-ils publier leurs vulnérabilités ; et
- comment les évolutions du secteur privées pourraient-elles être utilisées dans le secteur public.

25. Mme Davis commence par souligner la difficulté pour certains Alliés de partager les informations sur les cyberattaques qu'ils ont subies, et en particulier sur la façon dont cette information a été obtenue. Elle souligne que tous les Alliés tireraient profit d'une meilleure coopération, mais qu'il est difficile de dire à quel point les gouvernements peuvent se permettre d'être transparents au sujet des cyberattaques. Concernant une réponse crédible que l'OTAN pourrait apporter si l'article 5 était invoqué, elle indique qu'aucune règle claire n'a été établie. Elle déclare qu'il importe de réfléchir à la façon de prendre des mesures de représailles tout en évitant l'escalade des attaques. En dernier lieu, elle déclare qu'il est très difficile de mettre en œuvre une politique et une structure transversales qui puissent s'appliquer à tous les membres, étant donné que toute réaction exige une intervention des forces de l'ordre à l'échelle nationale.

VIII. Examen du projet de rapport de la sous-commission sur les tendances technologiques et la sécurité sur *Intelligence artificielle : Impact sur les forces armées de l'OTAN* [088 STCTTS 19 F] par Matej TONIN (Slovénie), rapporteur

26. Le rapporteur **Matej Tonin** (SI) souligne que presque tous les experts de la défense s'accordent pour dire que l'utilisation de l'intelligence artificielle dans les forces armées pourrait avoir un impact à tous les niveaux des conflits armés. Dans son projet de rapport, M. Tonin souligne les opportunités et les difficultés liées à l'utilisation de l'IA dans la défense. Il indique, en premier lieu, que cette technologie pourrait accélérer la vitesse d'analyse et d'action et améliorer la qualité de la prise de décision. Il ajoute que les systèmes autonomes robotisés présentent de nombreuses qualités. L'IA permettrait aux systèmes robotisés d'être bien plus performants qu'ils ne le sont aujourd'hui. Ces opportunités pourraient obliger les pays à restructurer leurs forces armées et à changer leurs concepts opérationnels.

27. M. Tonin a abordé les principaux défis, techniques et moins techniques, que présente l'adoption de l'IA dans le secteur de la défense. M. Tonin en a identifié trois :

- le défi de l'investissement, étant donné qu'il est nécessaire de disposer de davantage de ressources pour développer des capacités en IA ;
- le défi de l'innovation, car les gouvernements doivent progresser dans l'adoption et l'intégration de technologies provenant du secteur privé non spécialisé dans la défense ;
- le défi de la main-d'œuvre, car les pays ont besoin de plus d'experts en IA et ont dû former à nouveau ceux qui travaillent déjà dans les forces armées.

28. M. Tonin mentionne également les questions morales, juridiques et éthiques liées à l'IA. Il déclare aux délégués qu'il a examiné la question des systèmes d'armes autonomes létaux, qui auraient la capacité de tuer sans véritable supervision humaine. Cependant, il souligne que ces armes n'existent pas encore et qu'aucun État ne prévoit de les développer. En outre, tous les membres de la communauté internationale s'accordent sur l'idée que les humains doivent maintenir un « contrôle digne de ce nom » sur tous les systèmes autonomes. L'interprétation que font les États de ce contrôle reste, cependant, une question essentielle que l'on doit continuer à se poser. Néanmoins, cette discussion ne doit pas éclipser les autres questions morales, juridiques et éthiques auxquelles les États doivent déjà répondre.

29. Le rapporteur de la STCTTS mentionne également quelques défis techniques. Ils portent souvent sur les données disponibles pour les systèmes d'IA, la quantité et la qualité de ces données étant les principaux « ingrédients » pour de bons algorithmes. Il met l'accent en particulier sur ce que l'on appelle la vulnérabilité de l'alimentation en données, ainsi que sur le problème de la fiabilité de celles-ci. M. Tonin aborde également la volonté de la Russie et de la Chine d'adopter l'IA dans leurs forces armées. Selon M. Tonin, les principaux enseignements de son rapport sont : premièrement, la nécessité pour les Alliés de garder un rôle de chefs de file en ce qui concerne les investissements dans l'IA appliqués à la défense et, deuxièmement, la nécessité de maintenir un écart technologique suffisamment faible entre les Alliés pour que celui-ci puisse être comblé par l'interopérabilité.

30. Une fois le débat ouvert, un délégué demande s'il est prouvé que d'autres acteurs internationaux ne développent pas d'armes complètement autonomes. Il demande également comment les États membres de l'OTAN peuvent s'imposer des restrictions, notamment en matière de politique industrielle ou de questions éthiques ou morales, au moment d'envisager de développer l'IA. Les autres délégués demandent si les pays devraient envisager des solutions basées sur de petits ensembles de données, car ceux-ci sont de plus en plus importants, et s'interrogent sur la meilleure façon de collecter des données fiables pour les applications de l'IA. La question de la confidentialité des données est aussi posée à de nombreuses reprises. Certains membres ont des opinions divergentes concernant l'IA et la possibilité qu'elle devienne réellement plus intelligente que les humains.

31. Le rapporteur explique qu'il est probable que certains acteurs aspirent à développer des armes complètement autonomes, mais qu'à ce jour, cela n'a pas encore été fait. En outre, il souligne qu'il importe que l'Alliance rappelle que les humains devraient garder un « contrôle digne de ce nom » sur toutes les machines. Il affirme que la confidentialité des données est essentielle. Il indique que les différents pays ont des réglementations et des approches différentes de la confidentialité et que cela peut présenter une difficulté. Il prône un niveau élevé de protection des données. Il termine en soulignant, à nouveau, l'utilité de l'IA pour les forces armées.

IX. Examen du projet de rapport spécial *La lutte anti-sous-marine de l'OTAN : reconstruire les capacités, se préparer pour l'avenir* [089 STC 19 F] de Leona ALLESLEV (Canada), rapporteure spéciale, présenté par Njall Trausti FRIDBERTSSON (Islande), vice-président de la STC

32. **Njall Trausti Fridbertsson** (IS) commence la présentation de ce rapport en soulignant le renforcement majeur des patrouilles de sous-marins russes dans les zones d'opération de l'OTAN. Il observe que de plus en plus de sous-marins russes sont équipés de missiles longue portée *Kalibr* à guidage de précision. Avec ce missile, la Russie menace non seulement les liaisons maritimes transatlantiques, mais peut aussi interdire l'accès aux littoraux européens. Il ajoute que le rapport met l'accent sur les risques concernant les câbles de communication sous-marins. D'autres tendances devraient préoccuper l'Alliance dans ce contexte. Les projets d'expansion de la Chine au niveau mondial vont de pair avec une hausse de ses investissements en matière de défense, notamment la modernisation de ses sous-marins. En parallèle, la Corée du Nord cherche à développer des sous-marins porteurs de missiles balistiques à tête nucléaire.

33. Au-delà des enjeux posés par les acteurs extérieurs, l'Alliance est confrontée à un grave déficit de capacités de lutte anti-sous-marine, selon M. Fridbertsson. Il s'agit d'un problème de court terme et de long terme. Le nombre de plateformes pertinentes a chuté et les capacités actuelles deviennent rapidement dépassées. Toutefois, il est encourageant de voir que les Alliés réagissent. Sur le long terme, les mers sont devenues plus bruyantes, étant donné l'augmentation du trafic maritime, mais les sous-marins sont plus difficiles à détecter. M. Fridbertsson ajoute que les Alliés doivent, par conséquent, mettre en œuvre de nouvelles technologies de capteurs et l'intégration de véhicules autonomes sans pilote dans leurs missions de lutte anti-sous-marine. Le projet de rapport souligne également qu'il importe d'accroître les investissements dans les équipements de lutte anti-sous-marine.

34. **Taner Yildiz** (TR) ouvre le débat en demandant que soit ajoutée dans le rapport une clarification relative à la Convention de Montreux concernant le régime des détroits. Il se mettra en contact avec le personnel de la commission pour faire une proposition formelle. Les discussions et les autres questions ont porté sur certains des points suivants :

- l'importance d'investir dans les bonnes capacités et dans leur optimisation face aux nouvelles menaces ;
- les menaces relatives aux câbles sous-marins : un point qui, à la demande de certains délégués, devrait être creusé dans le rapport final ;
- les capacités spécifiques de lutte anti-sous-marine, y compris les capacités sans pilote ; et
- des demandes de clarification et d'une mise à jour sur l'évolution des capacités nationales pour la version révisée du rapport à l'automne.

35. M. Fridbertsson remercie les membres pour leurs interventions. Il transmettra les commentaires et les questions au rapporteur. Il souligne, à titre personnel, la nécessité d'investir, de développer et d'améliorer les capacités de lutte anti-sous-marine de l'Alliance.

X. Table ronde sur *Le défi de la science et de la technologie en Chine* avec Helena LEGARDA, chercheuse associée, Institut Mercator sur la Chine (MERICS), Berlin, Allemagne et Jan-Peter KLEINHANS, directeur de projet sécurité IdO, *Stiftung Neue Verantwortung* (SNV)

36. Dans sa présentation, **Helena Legarda** explique d'abord pour quelles raisons l'Alliance a intérêt à accorder une attention accrue aux progrès technologiques de la Chine. Elle déclare que, dans sa quête pour devenir une superpuissance mondiale dans le domaine des sciences et des technologies, la Chine, dotée d'une armée capable de gagner des guerres, s'est fixé comme objectif de surpasser l'Europe et les États-Unis et de dominer la sphère technologique. Le système de parti unique a permis à Pékin d'adopter une approche gouvernementale pour combler l'écart technologique avec l'Ouest. D'après elle, le fait que tout soit décidé en haut lieu a permis à la Chine de mobiliser le secteur privé, le gouvernement, l'industrie et l'ensemble de

la société autour de ses objectifs. Il s'agit d'un résultat que l'Europe et les États-Unis ont bien du mal à obtenir. Par exemple, Google a mis un terme au projet Maven du département américain de la défense, qui utilise l'intelligence artificielle pour interpréter des vidéos et des images, car l'opinion publique était préoccupée par l'usage que les forces armées pourraient faire de cette technologie. La Chine, explique-t-elle, a encouragé l'innovation nationale à travers des plans industriels nationaux et gouvernementaux pour certains secteurs spécifiques avec des objectifs ciblant la localisation, la création de marchés et la productivité.

37. Elle indique que l'accès à l'innovation étrangère est une autre voie vers la suprématie technologique. Parmi les autres stratégies, on compte l'acquisition de talents, les exportations, l'investissement dans les entreprises étrangères et l'acquisition de ces entreprises. Mme Legarda conclut en soulignant la vitesse des progrès technologiques chinois, grâce à des processus imposés d'en haut. Elle déclare que les États membres de l'OTAN doivent développer des stratégies cohérentes pour promouvoir et protéger les innovations.

38. **Jan-Peter Kleinhans** souligne les deux principales raisons justifiant la controverse actuelle sur les réseaux 5G/Huawei. Premièrement, le manque de technologies fiables de l'information et de la communication (TIC) en général et, deuxièmement, la dépendance technologique de l'Ouest vis-à-vis de la Chine.

39. M. Kleinhans souligne qu'actuellement, il reste impossible de prouver qu'il n'y a pas de codes malveillants dans les équipements technologiques. Les méthodes de normalisation et de certification n'ont pas pu suivre le rythme du développement technologique. D'après lui, ce contexte oblige les pays à faire confiance à l'entreprise qui produit le dispositif pour corriger les vulnérabilités au fur et à mesure qu'elles sont découvertes. La mesure dans laquelle un pays peut faire confiance à un autre dépend de la juridiction dans laquelle opère le fournisseur. Avec les réseaux 5G, l'industrie et les sociétés deviendraient plus vulnérables. Il ajoute que, dans les recommandations récentes sur l'évaluation des risques des réseaux 5G, il a été suggéré de mener des évaluations sur l'état de droit dans les pays d'origine des fournisseurs potentiels. M. Kleinhans souligne que l'Ouest reste mal équipé pour élaborer des politiques raisonnables en matière de sécurité des TIC. Il précise que l'approche de la question des 5G sous le prisme de l'espionnage industriel ou du sabotage potentiel serait probablement inefficace.

40. M. Kleinhans signale l'importance des politiques de sécurité des TIC. Si les pays se méfient des stations de base Huawei, ils devraient également craindre les centres de données d'Alibaba à Francfort. Mais à partir de quand cette logique deviendrait-elle peu pratique ? Il rappelle, au sujet des efforts de l'UE sur les politiques des TIC, que la dépendance technologique vis-à-vis de la Chine pourrait se retourner contre l'UE dans de futurs conflits et différends commerciaux. L'UE devrait élaborer des politiques industrielles judicieuses et stratégiques pour renforcer son secteur des TIC sans en perturber la chaîne mondiale d'approvisionnement. Il conclut en déclarant qu'il faudrait davantage tenir compte de la dépendance technologique, un domaine dans lequel l'UE et l'Ouest pourraient élaborer des politiques stratégiques.

41. Les questions et observations des délégués portent notamment sur les points suivants :

- Comment les pays devraient-ils aborder les questions liées à la 5 G/Huawei ?
- Quelle serait l'efficacité de la nouvelle politique technologique du président américain Trump à l'égard de la Chine et quelles en seraient les conséquences probables à long terme ?
- La Chine pourrait-elle utiliser sa part du marché des minéraux des terres rares, essentiels pour les technologies de l'information et de la communication, pour exercer des pressions sur d'autres pays ?
- Comment la relation entre Google et Huawei se développera-t-elle à l'avenir ?
- Comment l'UE pourrait-elle stimuler une croissance innovante ?

- La Chine pourrait-elle gagner une avance technologique sur l'Alliance ?
- L'OTAN devrait-elle se repositionner vis-à-vis de la Chine ?

42. Mme Legarda souligne que le cas de Huawei est très spécifique. Le Parti communiste chinois soutient l'entreprise, car 98 % de l'entreprise est contrôlée par le Parti. Elle souligne que le Parti est au-dessus des lois et que chaque entreprise et chaque individu chinois est tenu de collaborer avec les autorités lorsque le parti soulève des questions de sécurité nationale. Elle observe que, pour le Parti, le concept de sécurité nationale est très large. D'après elle, Huawei pourrait se comporter comme une entreprise privée pour le moment, mais répondre aux exigences du Parti si on le lui demande. Elle indique que la politique américaine actuelle montre clairement que la Chine est toujours dépendante des États-Unis, puisque cette politique a eu des répercussions négatives sur l'économie chinoise. Bien que cette politique ait mis à l'ordre du jour des questions cruciales, elle ne fera pas dévier la Chine de sa trajectoire sur le long terme. La Chine n'abandonnera pas ses politiques technologiques quelle que soit la politique américaine. La priorité de la Chine est de maintenir le statu quo. Pour atteindre son objectif, la Chine est prête à subir des conséquences économiques. Mme Legarda ne pense pas que les pourparlers entre les États-Unis, l'UE et la Chine puissent améliorer une situation devenue très idéologique.

43. En ce qui concerne la menace que représente la Chine pour l'approvisionnement en minéraux des terres rares, M. Kleinhans déclare que cette question particulière reste une question secondaire. La Chine est encore dépendante des États-Unis pour les puces électroniques et a surestimé ce moyen de pression spécifique.

44. Au cours de la discussion, Mme Legarda indique que Huawei a déjà investi dans la création de son propre système d'exploitation, car la société avait anticipé le risque d'être exclue d'Android et d'iOS à un moment donné. Toutefois, souligne M. Kleinhans, Huawei est encore loin derrière Apple, Google et Microsoft. D'après lui, la Chine a compris la nécessité de devenir plus indépendante et, en représailles, avait publié sa propre liste d'entreprises « occidentales » qui ne sont pas dignes de confiance. Mme Legarda avertit également que certains efforts contre les entreprises chinoises pourraient nuire à la fois à la Chine et à l'« Ouest », car les chaînes d'approvisionnement sont fortement intégrées. En ce qui concerne l'avenir de l'innovation chinoise, Mme Legarda fait observer que l'innovation est certainement possible, mais que l'État chinois non démocratique et fermé reste un obstacle évident.

45. M. Kleinhans déclare que l'UE ne dispose d'aucune politique industrielle stratégique. Dans la mesure où la réglementation ne peut pas être imposée d'en haut et que les subventions ne seraient pas suffisantes, l'UE doit comprendre où elle se situe dans la chaîne d'approvisionnement des TIC. Elle doit élaborer des politiques de financement et de soutien aux petites et moyennes entreprises, car elles sont devenues des cibles faciles pour les acquisitions chinoises.

46. En ce qui concerne le repositionnement de l'OTAN, Mme Legarda souligne la nécessité de ne pas perdre de vue les menaces classiques tout en considérant la Chine comme un acteur mondial. La Chine est déjà en Europe, à travers des exercices militaires avec la Russie et des opérations de navigation en Méditerranée et en mer Baltique. Elle conclut qu'une présence conventionnelle dans le Pacifique n'est cependant pas nécessaire. M. Kleinhans ajoute que, d'un point de vue technologique, les pays et leurs armées et sociétés dépendent de plus en plus de la technologie et de l'utilisation des réseaux mobiles commerciaux. Il conclut que l'OTAN devrait se concentrer sur l'impact des TIC sur la sécurité internationale, et que les Alliés qui partagent les mêmes idées devraient bâtir des systèmes de sécurité plus résilients.

XI. Présentation des activités futures de la commission et de la sous-commission sur les tendances technologiques et la sécurité (STCTTS)

47. La présidente décrit les activités récentes et futures de la STC. Les membres de la commission sont briefés sur la récente visite à Singapour et sur l'impact que les inventions et innovations déstabilisantes peuvent avoir sur la défense et la sécurité, mais aussi sur le secteur civil.

48. En ce qui concerne les prochaines visites, la STCTTS se rendra à Londres et dans le sud de l'Angleterre du 17 au 20 juin. Cette visite sera axée sur les sciences et technologies de la défense, la cybersécurité et la défense, l'intelligence artificielle, l'apprentissage automatique et les mégadonnées, la lutte anti-sous-marine, la défense maritime et la sécurité. Enfin, la troisième visite pourrait avoir lieu à Norfolk, Virginie, et à Washington DC à la fin octobre/début novembre. Le Commandement allié transformation de l'OTAN, le nouveau Commandement des forces conjointes de l'OTAN-Norfolk et la deuxième flotte des États-Unis seront probablement des éléments de cette visite. Il s'agit d'un changement dans le programme d'activités de la STC, étant donné qu'il n'était plus possible, pour des raisons logistiques, de participer à un exercice de lutte anti-sous-marine au large des côtes du Canada.

XII. Divers

49. Cette session de printemps 2019 constitue la dernière réunion plénière de la présidente de la commission, Maria Martens, car elle a décidé de ne plus se présenter au Sénat des Pays-Bas. **Bruno Jorge Vitorino** (PT), vice-président de la STC, saisit cette occasion pour revenir sur sa carrière et lui rendre hommage. Au nom de la commission, M. Vitorino la remercie pour son excellente présidence de la STC et lui souhaite le meilleur dans la poursuite de ses activités.

XIII. Date et lieu de la prochaine réunion

50. Mme Martens rappelle aux membres que la prochaine réunion de la commission aura lieu à la session annuelle qui se tiendra à Londres en octobre.

XIV. Remarques de clôture

51. En conclusion de la réunion, la présidente remercie les membres et les intervenants pour leurs contributions constructives et la délégation slovaque et son personnel pour la bonne organisation de la session.

52. Elle remercie les interprètes, le directeur et la coordinatrice de la commission ainsi que les assistants de recherche chargés de prendre des notes. Enfin, elle clôt cette réunion de la STC de la session de printemps 2019.