167 STC 19 F rév. 1 fin
Original : anglais

RÉSOLUTION 459

sur

LE RENFORCEMENT DE LA CYBERSÉCURITÉ, LA CYBERDÉFENSE ET LA CYBERDISSUASION DE L'OTAN

L'Assemblée,

1. ***Consciente*** de la complexité croissante du paysage international des cybermenaces ;

2. ***De plus en plus confrontée*** à des cybercampagnes répétées situées juste en dessous du seuil du conflit armé et ***reconnaissant*** le rôle important de l'Alliance pour y faire face ;

3. ***Restant vigilante*** face à l'augmentation des cybermenaces émanant de groupes terroristes et extrémistes ;

4. ***Soulignant*** que les cyberattaques commises par des États ou leurs intermédiaires représentent la cybermenace la plus importante pour l'OTAN ;

5. ***Relevant*** que les cyberattaques peuvent constituer une menace pour la prospérité, la sécurité et la stabilité des pays et de la communauté euro-atlantique, et pourraient ainsi conduire à l'invocation de la clause de défense collective (article 5) du traité fondateur de l'OTAN ;

6. ***Précisant*** que chaque membre de l'Alliance a la responsabilité de maintenir et d'accroître sa capacité individuelle et collective de résistance à des cyberattaques, mais ***insistant*** sur le rôle crucial de soutien joué par l'OTAN ;

7. ***Insistant*** sur la mission défensive de l'OTAN, son attachement indéfectible au droit international et au principe d'un contrôle politique rigoureux des opérations militaires ;

8. ***Rappelant*** la nécessité d'opérer dans le cyberespace et d'y mener des actions de défense aussi efficacement que dans d'autres domaines militaires ;

9. ***Saluant*** les avancées récentes des Alliés et de l'OTAN en matière de renforcement de la cybersécurité, de la cyberdéfense et de la cyberdissuasion ;

10. ***Rappelant*** la difficulté d'attribuer les cyberattaques et ***soulignant*** le danger d'escalade et la nécessité pour les États de déterminer les réponses appropriées ;

* présentée par la commission des sciences et des technologies et adoptée par l'assemblée plénière le lundi 14 octobre 2019, Londres (Royaume-Uni)

11. **INVITE INSTAMMENT** les gouvernements et les parlements des pays membres de l'Alliance atlantique :

a. à respecter les engagements pris dans le cadre du processus OTAN de planification de défense ainsi que l'engagement en faveur de la cyberdéfense ;
b. à adopter une doctrine OTAN pour le cyberespace d'ici la fin 2019 ;

Cybersécurité et cyberdéfense

c. à redoubler leurs efforts concernant :
   i. le développement des cybercapacités ;
   ii. les dépenses en matière de cyberdéfense ;
   iii. l'adaptation des structures alliées et OTAN ;
   iv. l'intégration des effets cyber dans les opérations militaires ;
   v. l'amélioration des cyberstratégies et des cyberpolitiques au niveau des pays et de l'OTAN ;
   vi. la coopération et l'échange des meilleures pratiques ;
   vii. la connaissance de la situation, l'échange d'informations et l'évaluation ;
   viii. l'amélioration des compétences et du niveau de connaissance de tous les acteurs concernés des pays membres et de l'OTAN ;
   ix. la promotion des formations, des entraînements et des exercices ;
   x. le renforcement des cyberpartenariats efficaces avec l'industrie, les milieux universitaires, les pays partenaires et d'autres organisations internationales, en particulier l'UE dans le cadre du partenariat stratégique OTAN-UE ;

d. à envisager sérieusement la mise à disposition d'effets cyber offensifs et défensifs pour les opérations OTAN, sur la base du volontariat, si tel engagement n'a pas encore été pris ;

Cyberdissuasion

e. à continuer d'afficher leur détermination et leur crédibilité pour prévenir les cyberattaques ;

f. à maintenir une politique de cyberdissuasion ambiguë quant au seuil à partir duquel une cyberattaque est considérée comme une attaque armée et sur les potentielles réponses collectives si ce seuil venait à être franchi ;

g. à continuer de chercher à réduire les risques d'escalade par une communication et un dialogue diplomatiques clairs, un haut degré de transparence sur les cybercapacités et les politiques y afférentes, ainsi qu'à apporter un soutien à l'élaboration de normes et l'adoption de mesures visant à renforcer la confiance dans le cyberespace ;

Cybercampagnes répétées

h. à reconnaître le risque stratégique à long terme que représentent les cybercampagnes répétées, et intensifier les consultations au sein de l'Alliance et avec les partenaires aspirant à l'adhésion ;

j. à lutter contre les cybercampagnes répétées à l'aide d'une combinaison adaptée de mesures de sécurité, de défense et de dissuasion, y compris une préparation et une résilience accrues du secteur civil ;

k. à attribuer les cyberopérations malveillantes, dans la mesure du possible, dans un délai réduit, de façon coordonnée, tout en respectant la souveraineté des gouvernements ;

l. à continuer à affiner leurs stratégies de lutte contre les menaces hybrides.