SENATO DELLA REPUBBLICA

XVIII LEGISLATURA

Doc. XII-*quater*
n. 24

ASSEMBLEA PARLAMENTARE DELLA NATO

Risoluzione n. 459

Il rafforzamento della sicurezza, della difesa
e della deterrenza cibernetiche della Nato

Trasmessa il 12 novembre 2019

NATO PARLIAMENTARY ASSEMBLY

RESOLUTION n. 459

Strengthening Nato cyber security, defence, and deterrence (*)

THE ASSEMBLY,

1. *Recognising* the increasingly complex international cyber threat landscape;

2. *Increasingly facing* persistent cyber campaigns falling below the threshold of armed conflict and *acknowledging* an important role for the Alliance in countering them;

3. *Remaining vigilant* regarding increasing cyber threats from terrorist and extremist groups;

4. *Underlining* that cyber attacks by states or their proxies present the biggest cyber threat to NATO;

5. *Stressing* that cyber attacks can threaten national and Euro-Atlantic prosperity, security, and stability and could, thus, lead to the invocation of the collective defence clause (Article 5) of the NATO's founding treaty;

6. *Underscoring* that Allies have an individual responsibility to maintain and develop both individual and collective capacity to resist cyber attacks, but *highlighting* NATO's crucial support role;

7. *Emphasising* NATO's defensive mandate, its continued adherence to international law, and the principle of strong political oversight of military operations;

8. *Recalling* the need to operate and defend in cyber space as effectively as in other military domains;

9. *Lauding* recent Allied and NATO progress on strengthening cyber security, defence, and deterrence;

10. *Recalling* the difficulty of attributing cyber attacks and *stressing* the danger of escalation and the need for states to decide on appropriate responses;

11. *URGES* member governments and parliaments of the North Atlantic Alliance:

a. to fulfil their national cyber commitments under the NATO Defence Planning Process and the NATO Cyber Defence Pledge;

b. to adopt a NATO cyber space doctrine by the end of 2019;

(*) Presented by the Science and Technology Committee and adopted by the Plenary Assembly on Monday 14 October 2019, London, United Kingdom.

Cyber Security and Defence

c. to redouble their efforts on:

i. cyber capability development;

ii. cyber defence expenditures;

iii. adaptation of Allied and NATO structures;

iv. integration of cyber effects into military operations;

v. refinement of cyber strategies and policies at the national and NATO levels;

vi. cooperation and exchange of best practices;

vii. situational awareness, information sharing, and assessment;

viii. enhancement of skills and awareness across all national and NATO stakeholder communities;

ix. fostering education, training and exercises;

x. strengthening effective cyber partnerships with industry, academia, partner nations, and other international organisations, especially the EU as part of the NATO-EU Strategic Partnership;

d. to strongly consider making defensive and offensive cyber effects available for NATO operations on a voluntary basis, if not already committed to do so;

Cyber Deterrence

e. to continue to signal their resolve and credibility to deter cyber attacks;

f. to maintain a cyber deterrence policy of ambiguity concerning the threshold at which a cyber attack is considered an armed attack and possible collective responses if that threshold is crossed;

g. to continue to seek to reduce escalatory risks through clear diplomatic messaging and engagement, a high level of transparency on cyber capabilities and policies, and support to norm-development and confidence-building measures in cyber space;

Persistent Cyber Campaigns

h. to recognise the long-term strategic risk constituted by persistent cyber campaigns and intensify consultations within the Alliance and with partners with membership aspirations;

j. to counter persistent cyber campaigns with the right mix of security, defence, and deterrence, including increased civil preparedness and resilience;

k. to attribute malicious cyber operations, when feasible, in a timely and coordinated fashion while respecting the sovereignty of governments; and

l. to continue to refine their strategies for countering hybrid threats.

ASSEMBLÉE PARLEMENTAIRE DE L'OTAN

RESOLUTION n. 459

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;

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

(*) Présentée par la Commission des sciences et des technologies et adoptée par l'assemblée pléniere le lundi 14 octobre 2019, Londres (Royaume-Uni).

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.

ASSEMBLEA PARLAMENTARE DELLA NATO

RISOLUZIONE n. 459

Il rafforzamento della sicurezza, della difesa e della deterrenza cibernetiche della Nato (*)

L'ASSEMBLEA,

1. *Riconosciuta* la crescente complessità dello scenario internazionale delle minacce cibernetiche;

2. *Esposta sempre più spesso* a campagne cibernetiche persistenti collocate al di sotto della soglia del conflitto armato e *riconosciuta* l'importanza del ruolo dell'Alleanza per contrastarle;

3. *Costantemente vigile* per l'aumento delle minacce cibernetiche provenienti da gruppi terroristici ed estremisti:

4. *Sottolineato il fatto che* gli attacchi cibernetici da parte di Stati o di loro intermediari rappresentano per la NATO la più grande minaccia cibernetica;

5. *Evidenziato il fatto* che gli attacchi cibernetici possono minacciare la prosperità, la sicurezza e la stabilità euro-atlantiche e, quindi, potrebbero determinare l'invocazione della clausola di difesa collettiva (Articolo 5) del Trattato istitutivo della NATO;

6. *Sottolineato il fatto* che gli Alleati hanno la responsabilità individuale di mantenere e sviluppare la capacità sia individuale che collettiva di resistere agli attacchi cibernetici, ma *evidenziato* il cruciale ruolo di supporto della NATO;

7. *Evidenziati* il mandato difensivo della NATO, il suo perdurante rispetto del diritto internazionale e il principio del rigoroso controllo politico delle operazioni militari;

8. *Richiamata* la necessità di operare e svolgere azioni di difesa nello spazio cibernetico con la medesima efficacia degli altri ambiti militari;

9. *Accolti con favore* i recenti progressi degli Alleati e della NATO in merito al rafforzamento della sicurezza, della difesa e della deterrenza cibernetiche;

10. *Richiamata* la difficoltà di individuare gli autori degli attacchi cibernetici e *sottolineati* il pericolo di un'*escalation* e la necessità che gli Stati decidano le risposte appropriate;

11. *ESORTA* i governi e i parlamenti dei Paesi dell'Alleanza nord-atlantica a:

a. onorare gli impegni nazionali in materia cibernetica assunti nell'ambito del Processo NATO di Pianificazione della Di-

(*) Presentata dalla Commissione Scienza e Tecnologia e adottata dall'Assemblea Plenaria a Londra, Regno Unito, lunedì 14 ottobre 2019.

fesa e dell'Impegno NATO per la Difesa Cibernetica;

b. adottare una dottrina NATO sullo spazio cibernetico entro la fine del 2019;

Sicurezza e Difesa Cibernetiche

c. raddoppiare il proprio impegno in materia di:

i. sviluppo delle capacità cibernetiche;

ii. spese per la difesa cibernetica;

iii. adattamento delle strutture degli Alleati e della NATO;

iv. integrazione degli effetti cibernetici nelle operazioni militari;

v. affinamento delle strategie e delle politiche cibernetiche a livello nazionale e a livello NATO;

vi. cooperazione e scambi di migliori pratiche;

vii. conoscenza della situazione, condivisione di informazioni, valutazioni;

viii. potenziamento delle competenze e sensibilizzazione all'interno di tutte le comunità dei soggetti portatori di interessi a livello nazionale e a livello NATO;

ix. promozione dell'educazione, dell'addestramento e delle esercitazioni;

x. rafforzamento di partenariati cibernetici efficaci con l'industria, il mondo accademico, le nazioni *partner* e altre organizzazioni internazionali, in particolare l'UE come parte del Partenariato Strategico NATO-UE;

d. valutare concretamente la possibilità di rendere disponibili per le operazioni NATO, su base volontaria, gli effetti cibernetici difensivi e offensivi, qualora non si siano già assunti impegni al riguardo;

Deterrenza Cibernetica

e. continuare a mostrare la propria determinazione e credibilità in materia di deterrenza cibernetica;

f. mantenere una politica di deterrenza cibernetica ambigua con riferimento alla soglia oltre la quale un attacco cibernetico sia considerato un attacco armato e alle possibili risposte collettive in caso di superamento di quella soglia;

g. continuare a cercare di ridurre i rischi di *escalation* attraverso una comunicazione e un dialogo diplomatico chiari, un alto grado di trasparenza sulle capacità e sulle politiche cibernetiche, e il sostegno a misure che favoriscano lo sviluppo di norme e il rafforzamento della fiducia nello spazio cibernetico;

Campagne Cibernetiche Persistenti

h. riconoscere il rischio strategico a lungo termine rappresentato dalle campagne cibernetiche persistenti e intensificare le consultazioni all'interno dell'Alleanza e con i *partner* che aspirano all'adesione;

j. contrastare le campagne cibernetiche persistenti con una giusta combinazione di sicurezza, difesa e deterrenza, ivi incluso un più alto livello di preparazione e resilienza a livello civile;

k. individuare gli autori delle operazioni cibernetiche malevole, quando possibile, in modo tempestivo e coordinato, rispettando la sovranità dei governi; e

l. continuare ad affinare le proprie strategie di contrasto alle minacce ibride.

180124085430