NATO PARLIAMENTARY ASSEMBLY

167 STC 19 E rev. 1 fin.
Original: English

RESOLUTION 459

on

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;

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

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;

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.