NATO PARLIAMENTARY ASSEMBLY

COMMITTEE ON DEMOCRACY AND SECURITY
166 CDS 22 E rev. 1 fin | Original: French

STRENGTHENING THE CYBER RESILIENCE OF ALLIED SOCIETIES[1]
RESOLUTION 475

The Assembly,

1. ***Acknowledging*** the essential contribution of digital technologies to the functioning, well-being, cohesion and security of Allied societies;

2. ***Concerned*** about the growth, sophistication and increasingly destabilising impact of malicious cyber activities targeting all sectors, including public services, private companies and democratic institutions;

3. ***Commending*** efforts made in recent years by Allies and NATO to enhance their capacity to prevent, deter and counter malicious cyber activities; and ***welcoming*** the emphasis on combatting the latter and commitments made in NATO's new Strategic Concept;

4. ***Alarmed*** by the aggressive and irresponsible behaviour of authoritarian states in cyberspace; and ***concerned*** by the multiplication and diversification of malicious non-state cyber actors, their objectives and their techniques;

5. ***Strongly denouncing*** the unacceptable proliferation of malicious cyber activities against critical civilian infrastructure in Ukraine before and during Russia's new illegal and unprovoked invasion of the country, and ***recognising*** the importance of Allied support to Ukrainian authorities in thwarting them;

6. ***Reaffirming*** that Allies have a duty to maintain and strengthen their national cyber resilience and that NATO can provide support in this regard, notably through the Cyber Defence Pledge;

7. ***Stressing*** that NATO has recognised cyberspace as an operational domain; and ***reiterating*** the possibility for the North Atlantic Council to decide, on a case-by-case basis, when a cyber-attack would lead to the invocation of Article 5;

8. ***Reaffirming*** the crucial role of partnerships in combatting cyber threats that defy borders, and ***welcoming*** the extensive and effective cooperation between NATO and the European Union (EU) in this area;

9. ***Recalling*** that enhancing the cyber security of Allied societies cannot be achieved at the cost of undermining the democratic freedoms, rights and principles that underpin them;

10. ***Noting*** that the international community has recognised the applicability of international law in cyberspace, and ***reiterating*** the Alliance's commitment to its observance in order to promote a free, open, peaceful and secure cyberspace;

---

1 Presented by the Committee on Democracy and Security and adopted by the Plenary Assembly on Monday 21 November 2022

11. **URGES** the member governments and parliaments of the North Atlantic Alliance and, where appropriate, NATO bodies:

a. to swiftly implement agreed-on common policies, notably the Cyber Defence Pledge, the Comprehensive Cyber Defence Policy and the new Strategic Concept;

b. to enhance cyber deterrence and defence capabilities:
   i. by being transparent about their action doctrines;
   ii. by consolidating their ability to quickly and effectively coordinate their responses, in particular concerning attribution, to cyber activities while respecting Allies' national competence ;
   iii. by reserving the right to voluntarily adopt joint measures against perpetrators of cyber operations below the threshold at which they would be considered armed attacks warranting a military response;
   iv. by taking action and developing cyber capabilities – including, at the national level, offensive capabilities – and greater interoperability to enable Allies to impose significant costs on perpetrators for their malicious cyber activities;

c. to deepen understanding of cyber threats, intelligence sharing and research, for example through the creation of dedicated applications for the general public, and to invest in network security in order to better prepare for and thwart malicious cyber activities;

d. to strengthen national policies and legal frameworks for combatting cyber threats and to continue working towards the development and implementation of international standards for responsible behaviour in cyberspace;

e. to intensify cooperation with relevant international organisations, notably the EU, partner countries, industry and academia, in particular by consolidating the exchange of information and best practices;

f. to raise awareness among all societal actors of their individual role in collective cyber resilience; to deepen collaboration with all private sector actors; and to strengthen civil-military cooperation in the cyber domain;

g. to maintain and increase support for partner countries facing cyber risks, in particular Ukraine, in order to counteract the irresponsible malicious cyber activities against the latter in the context of Russia's escalating war of aggression ;

h. to pursue and strengthen the regular organisation of exercises and training involving all the actors concerned, aimed at identifying their cyber vulnerabilities and testing and developing their individual and collective capacity to react to and recover from malicious cyber activities;

i. to ensure that parliaments, civil society and the public have all the information and means necessary to monitor measures aimed at enhancing cyber security to make sure that these do not infringe on democratic values or individual rights.