North Atlantic Council

Distr.: General
18 June 2026

Original: English

Resolution 2026/0000

Resolution adopted by the North Atlantic Council on 18 June 2026

Strengthening NATO's Response Against Hybrid Warfare Including Cyber Attacks and Drones

The North Atlantic Council,

Alarmed by the recent surge in grey zone provocations against NATO (North Atlantic Treaty Organization) members,

Noting with deep concern the rapid increase of cyber warfare and disinformation used against NATO members,

Convinced of the endangerment of critical infrastructure, military supply chains and democracy caused by such means of warfare,

Recognizing the disconnected approach towards the security of NATO member states,

Fully aware of the difference in geographical, political and economic situation as well as military preparedness between NATO member states,

Deeply regretting that a joint agreement on the conditions for the invocation of article 5 as well as for measures to be taken in such a case has not been established,

Emphasizing the importance of civil preparedness,

Viewing with appreciation the successful implementation of missions such as Eastern Sentry,

1. **Calls for** prioritizing operational NATO joint procurement, production and research including but not limited to:
    (a) establishing a coordinated stockpile for high-consumption items via pooled purchasing with:
        (i) the total budget and items to be bought being established collectively by the member countries with final approval of the North Atlantic Council,
        (ii) the number of financial resources contributed by each NATO member being established using the countries proportion of total NATO GDP (Gross Domestic Product),
        (iii) the storage of these items being distributed according to risk assessment, logistics and front-line-needs among member states,

(b) the standardization of Counter-Unmanned Aerial Systems (c-UAS) and intelligence systems,
(c) encouraging weaponry trade and cooperation in research and development,
(d) providing technical and financial support to allies when needed;

2. **Approves of** the decision of every NATO member being obligated to invest a minimum of 5% of their GDP annually into its own defence and deterrence by 2035;

3. **Seeks to** deepen NATO coordination by:
(a) introducing mandatory annual meetings between all Ministers of Foreign Affairs and all Ministers of Defence of all NATO member states,
(b) mandating annual NATO summits,
(c) maintaining regular consultations on defence policy and responses to hybrid threats,
(d) providing the NATO Defense College Foundation with an annual budget of $2M;

4. **Requests** urgent NATO actions to counter hybrid threats by:
(a) prepositioning c-UAS and intelligence systems in vulnerable member states,
(b) expanding the frequency and scope of joint exercises,
(c) establishing a NATO innovation fund for hybrid warfare to promote research and development in new
(d) technologies, where each member state is required to invest between 0,25 - 0,4 percent of their GDP;

5. **Encourages** member states to increase civil readiness by:
(a) protecting critical infrastructure and diversifying supply chains,
(b) enhancing community preparedness and raising awareness through measures such as:
(i) public campaigns,
(ii) volunteer training,
(iii) strengthening media literacy programs against disinformation,
(c) improving logistics and medical treatment capacities,
(d) improving civil preparedness in case of an emergency through measures like emergency plans, public
(e) warning systems and stronger civil protection mechanisms;

6. **Further** requests to establish a joint Rapid Hybrid Response Task Force (RHRTF) to respond to hybrid provocations and attacks that:
(a) disrupts and neutralizes cyber and drone-related threats or other hybrid threats through defensive
(b) measures, intelligence cooperation, and authorized operations in accordance with international law,
(c) is limited to assisting attacked nations unless Article 5 is invoked,
(d) enhances attribution frameworks to rapidly and accurately identify the countries or organizations
(e) responsible,
(f) has access to intelligence and resources shared by and between NATO members;

7. **Calls for** the introduction of protocols for coordinated responses against hybrid attacks and sabotage including, but not limited to:
(a) counterattacks by RHRTF after a decision to invoke Article 5,
(b) positioning of equipment and personnel into concerned member states,
(c) economic sanctions that:
(i) sanction goods dependent on the country affected,
(ii) amount to at least 2% of the country's GDP;

8. **Further proclaims** the need to contribute to missions such as the Eastern Sentry;

9. **Recommends** to all remaining member states to join the NATO Cooperative Cyber Centre of Excellence (CCDCOE) and to maintain full collaboration within the framework of the NATO Integrated Cyber Defence Centre (NICC) and the Hybrid CoE and also urges all members to adopt minimum security standards for the cyber security of critical infrastructure;

10. **Strongly condemns** all military actions or operations not in line with International Law or the UN (United Nations) Charta;

11. **Seeks** the formulation of non-kinetic Rules of Engagement (RoE) for NATO, outlining proportional, pre-authorized cyber and economic countermeasures that can be deployed defensively to neutralize attackers' offensive capabilities without causing accidental military escalations;

12. **Proposes** the establishment of a secure NATO Joint c-UAS and Maritime Sensor Network to:
    (a) unify drone and electronic jamming detection,
    (b) deploy permanent acoustic, optical, and other types of under- and overwater sensors to detect drone and underwater attacks before they cause actual harm,
    (c) integrate surveillance data into NATO's air and missile defense systems;

13. **Strongly affirms** that infrastructure including pipelines and undersea cables is to be more strictly monitored and inspected frequently to ensure the protection of submarine cables in affected sea region;

14. **Calls for** the establishment of a Black Sea Hybrid and other waters controlled by the NATO Threat Monitoring Initiative involving Bulgaria, Romania, and Türkiye to enhance maritime surveillance, cybersecurity coordination, intelligence-sharing, and early-warning capabilities by:
    (a) establishing a Joint Black Sea Hybrid Threat Coordination Center responsible for collecting, analyzing, and disseminating information on hybrid threats, while facilitating regular intelligence-sharing among participating states and NATO liaison officers,
    (b) integrating maritime surveillance systems, coastal radar networks, satellite imagery, tracking into a shared real-time monitoring platform to detect suspicious activities, unauthorized military operations, and threats to critical infrastructure,
    (c) creating a secure cyber information-sharing network and enhancing cooperation with NATO Centres of Excellence to improve cyber defense capabilities, exchange threat intelligence, and counter disinformation campaigns,
    (d) organizing annual multinational exercises and deploying AI-supported early-warning mechanisms to strengthen preparedness against cyberattacks, GPS (Global Positioning System) interference, sabotage operations, and other forms of hybrid warfare,
    (e) protecting critical Black Sea and other waters controlled by the NATO energy and communication infrastructure through coordinated monitoring, risk assessments, emergency response planning, and financial, and technical assistance from NATO Allies,
    (f) deploying a trilateral early-warning mechanism jointly operated by Bulgaria, Romania, and Türkiye, utilizing artificial intelligence and data analytics to identify emerging hybrid threats in the Black Sea region and provide timely alerts to national authorities and NATO command structures;

15. **Requests** the intensification of the Planning and Review Process (PARP) to specifically enhance the interoperability, coordination, maritime security, and information-sharing of Counter-Unmanned Aerial Vehicle capabilities across all Allied forces;

16. **Calls for** the development of clear criteria for defining the attacks that may lead to an invocation of Article 5 of the North Atlantic Treaty, including attacks that:
    (a) cause significant and sustained disruption to critical national infrastructure, including energy, water, healthcare, financial, or communication systems, thereby substantially impairing the functioning of a member state,
    (b) constitute a coordinated hybrid operation involving multiple actors, multiple member states, or the simultaneous use of different means of attack, resulting in a significant threat to the security of one or more NATO member states,
    (c) attack NATO operational infrastructure, including military bases, command-and-control facilities, communication systems, or ongoing NATO missions and operations;

17. **Calls for** a better protection for islands and their populations with military, civil, and technological measures to be taken to counter hybrid threats in these often isolated regions such as, but not limited to:
    (a) Laying alternative cable routes, expanding satellite internet and improving alternative power supplies and especially gas infrastructure for quick response to hybrid attacks,
    (b) focused on building a better stockpile in case of emergency, such as military and civilian materials,
    (c) desensitizing the population to misinformation regarding take overs.

Vote result	Adopted	
	In favour:	Clauses voted on individually
	Against:	Clauses voted on individually
	Abstentions:	Clauses voted on individually
Date of vote	18 June 2026	
Final editor	Laura Petra Blümel	