



North Atlantic Council

Distr.: General
19 June 2026

Original: English

Resolution 2026/0002

Resolution adopted by North Atlantic Council on 19 June 2026

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

The North Atlantic Council,

Noting the rapid development of the Internet and cyber technologies with deep concern,

Alarmed by the great harms caused by the use of cyber attacks and drones in the ongoing Russia-Ukraine war and in the Gaza conflict,

Deeply concerned by the European as well as NATO's (North Atlantic Treaty Organization) continental and cyber security being threatened by the Russian aggression on Ukraine,

Having adopted several multilateral military cooperations of enhancing cyber resilience and resistance such as "Cyber Range Connect 2025",

Fully aware of the merely 2 percent of NATO allies' defense spending in comparison to dictatorships China and Russia,

1. **Calls for** a NATO Hybrid Warfare framework for the sake of cybersecurity of NATO allies in which:
 - (a) NATO Defense College Foundation provides funding to NATO allies with closer boarder to Russia and GNI per capita under 60 000 USD to help them develop cyber technologies enhancing their cyber resilience,
 - (b) NATO organizes a military cooperation of strengthening cyber resilience between all NATO member states twice a year, based on the "Cyber Range Connect 2025" between Slovenia and Croatia which is ought to establish proportionating measures to guarantee safety of civilians,
 - (c) NATO member states with advanced cyber warfare defense capabilities must unconditionally provide their technology to other lagging members;
2. **Strongly urges** every NATO member state to impose more economic sanctions against Russia and China to prevent an escalation of Hybrid Warfare in Ukraine, for Russia has launched cyber attacks on Ukraine with Chinese aid such as Chinese drones;
3. **Urges** every NATO member state to accelerate the process of elevating their total defense and security expenditures to 2 percents of GDP by 2035 as decided at the 2025 NATO Summit in The Hague due to the high potential expenditures on developing cyber technologies;

4. **Strongly urges** NATO to take full responsibility in case of a hybrid warfare by but not limited to;
 - (a) counter-attacking a hostile nation's critical infrastructure in self-defense,
 - (b) economically and geopolitically sanctioning the attacking nations including the allies of the attacking nation;
5. **Proposes** all NATO member states to implement a labeling system in social media to prevent foreign hostile propaganda;
6. **Proposes** all NATO member states to prevent drone attacks by:
 - (a) deploying Directed-Energy Weapons (DEW) or Counter-Unmanned Aircraft Systems (C-UAS),
 - (b) establishing a protocol for the detection, identification and neutralization of drones and stress the importance of multinational collaboration; (passed automatically)
7. **Supports** a dedicated Atlantic Infrastructure Protection Framework (AIPF) which shall:
 - (a) extend the existing Baltic Sea Protection efforts to Atlantic corridors with particular potentials to infrastructure passing through or near the Azores,
 - (b) cover all form of critical infrastructure including submarine cables off-shore energy platforms and major port facilities,
 - (c) establish clear protocols for rapid investigation and response to suspected acts and sabotages or disruption,
 - (d) enhance digital skills to protect maritime security;
8. **Urges** all allies to work closer together on the problem of illegal migration as a form of hybrid warfare while respecting and relying on existing international rights;
9. **Supports** any further ideas, measures and strategies which can be helpful in the problem-solving process.

Vote result	Adopted
	<i>In favour:</i> Clauses voted on individually
	<i>Against:</i> Clauses voted on individually
	<i>Abstentions:</i> Clauses voted on individually
Date of vote	19 June 2026
Final editor	Laura Petra Blümel