PODCAST hybrid threats

Voice 1: Brian

Voice 2: Sarah

JINGLE to open intro to podcast

VOICE 1

You're listening to the European Parliamentary Research Service podcast on EU-NATO cooperation on countering hybrid threats.

VOICE 2

Propaganda wars, cyber-attacks, resource scarcity, migratory pressures… modern security threats are no longer of a military nature alone, but involve a mix of challenges, actors and means which make them increasingly complex…

VOICE 1

The need to counter these hybrid threats has pushed the EU and NATO to strengthen their capabilities and work closer together. Want to know more? Stay with us!

JINGLE TO START REAL CONTENT

VOICE 2

The concept of hybrid threat is not a new one, but it has gained more traction with recent conflicts in Syria and Ukraine. Today, adversaries use ambiguity and hybrid tactics to achieve their strategic objectives, blurring the traditional distinction between war and peace and limiting the opportunity for counter-attacks.

VOICE 1

In addition to intentional actions by state and non-state actors, new threats deriving from natural developments are an increasing source of concern. In the near future, extreme weather conditions and resource scarcity could provoke new conflicts between states over access to water and food, and drive millions into a climate exodus that could destabilise entire continents…

VOICE 2

Amidst this changing global security environment, the concept of hybrid threat embraces the interconnected nature of today's challenges, the multiplicity of actors involved and the available instruments: from military forces to diplomacy, humanitarian aid to economic development and technology. Because of their complexity, hybrid threats challenge the very nature of concepts like sovereignty, legitimacy and legality… And enforcing them is not easy…

VOICE 1

So how have two of the international organisations most concerned, the European Union and NATO, adjusted to this new security environment? Let's begin with the hard power… **MUSIC JINGLE**

VOICE 2

NATO's Article 5 is the cornerstone of the alliance's commitment to self-defence. It considers an armed attack against one member as an attack against all, triggering a collective response to protect the Alliance.

VOICE 1

This principle works as long as the attack can be proved and the culprit identified… which is easier in the case of military aggression, but how can we point the finger at a specific state for a cyber-attack conducted by hackers operating from around the world?

VOICE 2

Operating in the grey area between what is legal and illegal under international law, hybrid threats make it difficult to determine legal breaches and to establish responsibilities… This is why NATO members have increased consultations in the framework of Article 4, which can be triggered when a member feels its territorial integrity or security are under threat.

VOICE 1

This article was invoked by Poland in March 2014 as a result of the conflict in Eastern Ukraine, and most recently by Turkey after the terrorist attacks in Suruc. So, aware that hard-power alone will not suffice to win modern wars, NATO adopted a comprehensive approach to crisis management that blends all relevant actors and available instruments: military forces, diplomacy, political processes, economic development, and technology.

VOICE 2

It also extended the application of Article 5 to cyber-attacks, acknowledging the readiness to counter hybrid warfare as part of its collective defence principle, although the targeted nation still bears the main responsibility to respond to hybrid threats.

VOICE 1
But how has the EU adjusted to this new security environment? Let's move from the hard to the soft power…
MUSIC JINGLE

VOICE 2
In April 2016, the European Commission adopted a joint framework bringing together all relevant actors, policies and instruments to both counter and mitigate the impact of hybrid threats.

VOICE 1
The new framework focuses on improving situational awareness andbuilding resilience by addressing strategic sectors such as cybersecurity, critical infrastructure, the financial system, public health, food security, and tackling violent extremism.

VOICE 2
It strengthens the ability of member states and the Union to prevent, respond to crisis and recover in a coordinated manner.

VOICE 1
To counter hybrid threats more effectively, the EU has also decided to deepen its partnership with NATO. This was confirmed both in the EU's Global Strategy of June 2016 and the joint declaration adopted during NATO's Warsaw Summit a month later.

VOICE 2
The EU-NATO declaration identifies new areas of cooperation to deal with hybrid threats, in particular through building resilience, situational awareness and strategic communications. Cooperation in these areas is also mentioned in the EU Playbook, which is a sort of operational protocol for countering hybrid threats.

VOICE 1
But has cooperation between the EU and NATO moved from words to action? Let's look at the case of cyber defence. **MUSIC JINGLE**

VOICE 2
As the US presidential elections showed, cyber-attacks are a new weapon that can change the course of a nation… Aware of this power, both the EU and NATO have gradually built up their cyber-defence capabilities. Their cooperation started in 2010, though it really gathered speed with the high-level consultations held since January 2015.

VOICE 1
An important milestone was the signing of the Technical Agreement between the EU and NATO , which facilitates technical information-sharing to improve cyber incident prevention, detection and response in both organisations.

VOICE 2
The EU-NATO joint declaration also highlighted the need to expand coordination on cyber security and defence. But how?

VOICE 1
Well, at the end of 2016, EU and NATO ministers agreed on a list of concrete measures, such as strengthening cooperation on training and cyber exercises and fostering joint research and technological innovation in the field of cyber defence. And there's a whole list of actions to be implemented before the end of 2017!

VOICE 2
What's clear, as many researchers, have pointed out, is that countering hybrid threats from the East and the South requires a coordinated response from both NATO and the EU, transmitting the same strategic message to their challengers and agreeing on a set of common criteria for response…

VOICE 1
In this new security environment, the basic premise for closer EU-NATO cooperation is that effective response and resilience against hybrid threats require a mix of military and non-military capabilities. And given that hybridity assumes operations below the threshold of armed conflict, the EU's soft power is particularly valuable…

VOICE 2

And it’s here, in areas such as emergency response, counter terrorism, border management or energy security where the European Parliament can make its mark… In November 2016, the Parliament welcomed the Joint Framework on countering hybrid threats, highlighting the need to ensure the right balance between military and non-military capabilities and instruments.

VOICE 1

The truth is that while countering hybrid threats requires a mix of soft and hard power, too close an alignment of the EU and NATO responses risks shifting the optics towards a military prism…

VOICE 2

Besides strengthening capabilities in different areas, the key to countering hybrid threats may well lie in working together with different partners, and allowing everyone to do what they do best!

VOICE 1

You are listening to the European Parliamentary Research Service podcasts.

MUSIC JINGLE TO CONCLUDE