NATO'S STRATEGIES FOR RESPONDING TO HYBRID CONFLICTS

The North Atlantic Treaty Organization (NATO) has a long relationship with the hybrid. Initially used to describe a form of warfare that incorporates both conventional and irregular elements, NATO's current conception is based on the coordinated and synchronised use of different kinds of power that remain below the threshold of conflict. Hybrid threats are now established as a danger to the allies' security. The Strategic Concept approved at the Madrid Summit in 2022 warns of China and Russia's use of hybrid threats and their effects, even to the point of potentially leading Article 5 of the Washington Treaty to be invoked.

Guillem Colom Piella
Full Professor of Political Science, Pablo de Olavide University

CIDOB REPORT
08- 2022

The origins

Influenced by hybrid warfare's rising popularity as a concept in the US strategic community following the 2006 Israel–Hezbollah war, and the appointment of General James Mattis to lead the Allied Command Transformation, NATO first showed an interest in hybrid warfare in 2007. Understanding that this form of warfare, in which «adversaries integrate conventional, irregular, terrorist, and criminal assets operationally and tactically», was likely to characterise conflict in the 21st century, the allies' means and capabilities needed adapting in order to operate effectively in these more ambiguous and diffuse settings. Unsurprisingly, then, hybrid tactics were included in the 12th capabilities planning review, were introduced into military testing campaigns, and figured among the Multiple Futures Project's recommendations for long-term transformation among the allies. While NATO military command did publish a basic concept to clarify the term and guide

this development of capabilities, the hybrid remained somewhat limited to the military field. This explains why, despite the «Albright Report» mentioning the hybrid on one occasion, it did not appear in the 2010 Strategic Concept. Other risks were mentioned, like terrorism, extremism, transnational crime and cyber-attacks, which had gained enormous prominence after the events in Estonia in 2007 and which would end up closely linked to the hybrid. The threat was not mentioned at the 2012 Chicago Summit either.

Despite the military interest in the hybrid, no consensus existed on the concept. In fact, the organisation's documents used war, threat, strategy and tactics interchangeably to refer to the complexity of 21st century conflicts. A political–military organisation like NATO was unprepared for such conflicts and had to address them via a «comprehensive approach» that would increase coherence between allied military actions and the civilian work of other actors in crisis management operations. In fact, many saw the intervention in Libya (2011) as an example of a conflict taking place outside the regular/irregular dichotomy (with government forces, guerrillas and mercenaries operating on ambiguous fronts), whose satisfactory resolution could only be achieved through a comprehensive approach with better crisis management tools and increased capacity to provide military support for post-conflict stabilisation and reconstruction.

The hybrid emerges

It was not until Russia's annexation of Crimea (2014) that public opinion and the political classes in NATO countries began to pay attention to hybrid threats. An astonished international community watched on as unmarked military units and local actors took the peninsula. Exploiting the region's sociopolitical divisions and launching a multi-channel disinformation campaign inside and outside Ukraine, Moscow managed to conceal its objectives and plausibly deny responsibility until the invasion was complete. The Russian incursion in Donbas (2014–) confirmed this blurring of the boundaries between peace and war into a large grey zone that was a natural habitat for misinformation and cyber-attacks. Since that time, these asymmetric, ambiguous tools, which are difficult to attribute and can impact society as a whole, have been observed by both NATO and the European Union.

Events in Ukraine helped the hybrid reach the top of the allied agenda. Described by NATO Secretary General Jens Stoltenberg as «the dark reflection of our comprehensive approach» these new challenges, which employ «a wide range of overt and covert military, paramilitary, and civilian

measures … in a highly integrated design», featured prominently at the Wales Summit (2014). At the meeting, it was agreed that tools should be developed to deter and respond to so-called «hybrid war threats» and to strengthen national capacities. Several of the initiatives set out there – reinforcing strategic communication, conducting exercises with hybrid scenarios, improving coordination with other organisations and drawing up a plan to counteract them – would be consolidated later. NATO's Strategic Communications Centre of Excellence, established in Riga in January 2014, became one of the organisation's pillars for combating disinformation and propaganda. Some months later, the first exercise began with a scenario that included hybrid threats in order to train allied politicians, officials and military personnel in these ambiguous situations that have the potential to paralyse decision-making. Many of those will end up benefitting from EU participation and this will become a key area of cooperation between the two organisations.

LIKE CYBER-ATTACKS, HYBRID STRATEGIES ARE AMBIGUOUS IN ORDER TO HINDER DETECTION AND ATTRIBUTION. THEY OPERATE BELOW THE VICTIM'S RESPONSE THRESHOLD. THE AFFECTED COUNTRY MUST ALLOCATE RESPONSIBILITY (ALTHOUGH IT CAN BE COMMUNICATED JOINTLY) AND ASSESSMENT IS MADE ON A CASE-BY-CASE BASIS. IT MAY THEREFORE BE DIFFICULT TO REACH THE CONSENSUS REQUIRED TO INVOKE ARTICLE 5.

In 2015, NATO presented its strategy for countering hybrid threats. Intended to guide its political and military efforts to combat hybrid threats, it was articulated around preparedness (identify, assess, communicate and attribute any activity in the grey zone), deterrence (strengthening allied societies' resilience, adapting the decision-making process and improving enlistment to reduce the impact of these threats, and increasing allied response options), and defence (increasing allied response capacity).

These initiatives were ratified and expanded at the Warsaw Summit in 2016. Describing hybrid warfare as «a broad, complex, and adaptive combination of conventional and non-conventional means, and overt and covert military, paramilitary and civilian measures … employed in an integrated manner by states and non-state actors to achieve their objectives», several agreements were reached. First, that the resilience of members' societies and infrastructure must be improved in order to reduce areas of exposure to hybrid strategies and to increase deterrence by denial. As with cyber defence, this is the member states' responsibility, with NATO's role to provide the necessary

support. This is logical, because every society has specific vulnerabilities that each grey zone is tailor-made to exploit, and a number of these hybrid tools (information-based, economic, cultural, legal, environmental, etc.) lie beyond the scope of NATO action. In any case, in 2018 anti-hybrid support groups were formed to provide technical assistance to countries – like Montenegro in 2019 – that need to prepare for or respond to hybrid threats.

Second, it was declared that a hybrid act may prompt the invocation of Article 5 of the Washington Treaty, under which an attack against any member of NATO is an attack against all. While this decision strengthens mutual defence, enables deterrence via punishment and increases the credibility of the process by altering the adversary's strategic calculations, implementing it may be more complicated than seems at first glance. Like cyber-attacks, hybrid strategies are ambiguous in order to hinder detection and attribution. They operate below the victim's response threshold. The affected country must allocate responsibility (although it can be communicated jointly) and assessment is made on a case-by-case basis. It may therefore be difficult to reach the consensus required to invoke Article 5. Instead, the consultation mechanism in Article 4 may be used, which allows any NATO member that believes its territorial integrity, political independence or security to be under threat to initiate a round of consultations with the other allies. Another factor is that NATO lacks the non-military tools to be able to give a gradual response, reducing its range of responses to hybrid attacks.

PREPARATION, DETERRENCE AND DEFENCE AGAINST THE COERCIVE USE OF POLITICAL, ECONOMIC, ENERGY OR INFORMATION TOOLS BY STATE ACTORS LIKE CHINA AND RUSSIA, OR BY NON-STATE ACTORS AND PROXIES, WHICH COULD PROMPT THE INVOCATION OF ARTICLE 5 OF THE WASHINGTON TREATY, HAVE BECOME ONE OF NATO'S FUTURE LINES OF ACTION.

Third on the list is collaboration with other actors facing similar problems. Since 2016, NATO has strengthened relations with Finland and Sweden (both have extensive experience countering hybrid threats using a comprehensive approach), Ukraine and Georgia (both are familiar with Russian activities that remain below the threshold of conflict), and several Indo-Pacific countries affected by China's grey zone activities. However, NATO's closest and most fruitful collaboration has been with the EU. The joint declaration signed between the organisations in Warsaw identified seven areas of cooperation, including the fight against hybrid threats, or

cybersecurity and cyber defence. Since then, the two organisations have collaborated to improve issues such as situational awareness, strategic communication, crisis response, resilience and cybersecurity. While the disparity in membership, organisational cultures and available tools makes closer cooperation difficult, both bilaterally and through the European Centre of Excellence for Countering Hybrid Threats, NATO and the EU have made significant progress in detection, attribution, response and resilience in this area.

Looking towards the future

In short, between the Wales and Warsaw summits, NATO laid the foundations for counteracting these strategies. Building on previous studies on hybrid warfare, since the 2014–16 period the organisation has made significant progress in combating this threat. Detection and early warning capabilities, threat intelligence, collaboration with other actors, exchange of sensitive information between members and with the EU, flexibility of decision-making processes, crisis response, strategic communication, cyber defence, support for national resilience and adapting deterrence to these more ambiguous environments in order to monitor escalation are just a few. While the invasion of Ukraine has shown that NATO's main *raison d'être* remains the deterrence and defence of its members against conventional or nuclear threats, the protection and resilience of its societies against these much more ambiguous threats will also be a key line of future NATO action. As the comprehensive approach and the lack of specific capabilities for civilian purposes show, NATO is a politico-military organisation with a much more limited catalogue of tools than the EU. However, its ability to deliver credible deterrence and response across the high threat spectrum makes it a good complement to an EU that is able to deploy a wide range of civilian tools.

Hybrid threats were barely mentioned in the final declaration of the London Summit (2019), while the Madrid Summit in June 2022 was monopolised by the invasion of Ukraine and the Russian threat to Euro-Atlantic stability. Nevertheless, these threats and the need to counteract them also played a prominent role at the meeting and in the Strategic Concept approved. Preparation, deterrence and defence against the coercive use of political, economic, energy or information tools by state actors like China and Russia, or by non-state actors and proxies, which could prompt the invocation of Article 5 of the Washington Treaty, have become one of NATO's future lines of action. This should come as no surprise, as the coming decade is likely to bring a rise in strategic revisionism and the proliferation of grey zones in which the hybrid will continue to play a fundamental role.

References

OTAN-Allied Command Transformation. *Multiple Futures Project. Navigating Towards 2030*. Norfolk: OTAN, 2009, p. 55.

OTAN. «Assured Security, Dynamic Engagement. Analysis and Recommendations of the Group of Experts on a New Strategic Concept for NATO» (17 May 2010a) (online) https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf

OTAN. «BI-SC Input to a New Capstone Project for The Military Contribution to Countering Hybrid Threats» (25 August 2010b) (online) https://www.act.nato.int/images/stories/events/2010/20100826_bi-sc_cht.pdf

OTAN. «Wales Summit Declaration» (5 September 2014) (online) https://www.nato.int/cps/en/natohq/official_texts_112964.htm

OTAN. «Jens Stoltenberg Keynote speech at the opening of the NATO Transformation Seminar» (25 March 2015) (online) https://www.nato.int/cps/en/natohq/opinions_118435.htm

OTAN. «Warsaw Summit Communiqué» (9 July 2016) (online) https://www.nato.int/cps/en/natohq/official_texts_133169.htm