NATIONAL INSTITUTE FOR PUBLIC POLICY

INFORMATION SERIES

HON. DAVID J. TRACHTENBERG, *Editor*
DR. MICHAELA DODGE, *Assistant Editor*
AMY JOSEPH, *Managing Editor*

Issue No. 448 November 4, 2019

NATO's Response to Hybrid Threats

Michael Rühle
Michael Rühle is Head, Hybrid Challenges and Energy Security, in NATO's Emerging Security Challenges Division.

The views expressed are the author's own.

Russia's annexation of Crimea in March 2014 was the greatest challenge for the post-Cold War European security architecture. After two decades of focusing on crisis operations abroad, NATO was forced to return to its original core task of collective defense, manifested, inter alia, in the rotational deployment of troops in the Alliance's East. However, Russia's approach in Ukraine also revealed that NATO needed to do more than enhancing its military posture. NATO also had to deal with the phenomenon of "hybrid warfare" - a type of warfare that combines overt and covert military and non-military means, and thus creates ambiguity that could severely complicate a unified response.

The concept of "hybrid warfare" is not new. What is new, however, is the seamless orchestration of military and non-military tools, as was demonstrated in Ukraine: Russia built up an impressive military threat close to Ukraine's borders, deployed paramilitary units, launched cyberattacks against Ukrainian infrastructure, interrupted gas supplies, and supported the East Ukrainian separatists with military equipment. This was accompanied by a

massive disinformation campaign intended to create the impression that Moscow had nothing to do with the events on the ground.

Arguably, given its internal weakness and its historical, cultural and economic ties with Russia, Ukraine presented a special case. Western countries are not likely to be as vulnerable as was Ukraine in 2014. Still, NATO allies recognized that a new era of conflict had dawned. Since NATO's success as a military alliance ultimately depends on the political cohesion of its allies, an opponent could undermine NATO's military preparations by focusing on dividing civil society (e.g. through fake news campaigns or election interference) and civilian infrastructure (e.g. cyberattacks), thus complicating NATO's collective decision-making process. Consequently, at their Wales Summit in September 2014 the allies pledged to prepare NATO for future hybrid threats.

A Strategy to Counter Hybrid Threats

At the same time, work began on a counter-hybrid strategy. This document, adopted in 2015, divides NATO's response to hybrid threats into three categories[1]:

Prepare

The Strategy is based on the assumption that defending against hybrid threats will become a permanent task for NATO. Hence, the first and foremost objective is to better understand the phenomenon of hybrid warfare. To this end, NATO continuously collects and evaluates information to identify seemingly unrelated events as hybrid campaigns and to identify their perpetrators. As hybrid attacks are directed primarily against states and governments, the responsibility for countering such attacks rests primarily with the states themselves. However, NATO can help allies identify national vulnerabilities and thus strengthen their resilience. The Strategy also highlights NATO's supportive role in areas such as civil emergency planning, critical infrastructure protection, strategic communications, cyber defense, energy security and counter-terrorism. The document also emphasizes the importance of exercises as a means to test decision-making processes.

Deter

Deterrence of hybrid threats is primarily about convincing potential opponents that the cost of their actions will exceed any reasonable gain. This can be achieved by measures taken by the broader international community (e.g. sanctions), but also by "naming and shaming" the attacker in order to deprive him of anonymity and to put him under political and moral pressure. NATO itself concentrates its efforts on further increasing the responsiveness of its armed forces and adapting its decision-making processes and command structures to the new circumstances.

Defend

In the initial phase, defense against a hybrid attack might be limited to the instruments used by the attacker, for example in cyberspace. The primary goal is to prevent a hybrid conflict from escalating to the military level. Should such an escalation nevertheless occur, the Alliance can also respond militarily. Like in the case of a traditional kinetic attack, NATO's response does not need to be confined to the geographical area in which the hybrid attack took place.

New Instruments for NATO

Since the release of NATO's Counter Hybrid Strategy, much of it has been implemented. An important step has been to improve intelligence sharing by establishing the Joint Intelligence and Security Division (JISD) in NATO's International Staff, which includes a unit specifically dedicated to analyzing hybrid threats. The JISD proved to be a successful bureaucratic innovation, not least because many allies have started to realize that hybrid threats can be both internal and external in nature, and are therefore increasingly willing to also share information on relevant domestic developments.

A further step towards a successful defense against hybrid threats is the deepening of relations between NATO and the European Union. Through informal cooperation at the working level, both institutions have developed "playbooks" to coordinate their respective responses to hybrid activities, and have started to engage in Parallel and Coordinated Exercises ("PACE"). The harmonization of the positions of both institutions is supported by the "European Centre of Excellence for Countering Hybrid Threats," established by Finland in 2016. Based in Helsinki, the Centre analyses hybrid threats but also serves as a forum for informal talks between NATO and EU staff.

NATO's exercises are also being adapted to the challenge of hybrid threats. By introducing hybrid elements into the scenarios, political and military decision-makers are forced to address the dilemmas that hybrid threats can pose, such as defining a threshold for eventual collective action in cases where an opponent's attacks stay below the kinetic level. These exercises have already revealed the difficulties of a military alliance in responding to non-kinetic attacks: if NATO were to wait with a collective response until an attacker employs kinetic means, a dangerous gap could emerge between aggression and reaction. Consequently, NATO needs to look much more closely into collective response options below the kinetic threshold.

Another important element of NATO's approach to tackling hybrid threats is the emphasis on allies' resilience. Since most hybrid attacks are aimed at individual nations, NATO must ensure that each member country is resilient enough to continue to perform as a reliable ally, for example, when NATO is preparing to send reinforcements during a crisis. The 2016 Warsaw Summit Declaration highlights resilience as the basis for credible deterrence and defense. In

line with this statement, allies pledged to improve their resilience to the full range of threats, including hybrid threats. While the strengthening of resilience is a national responsibility, NATO has produced guidelines that can serve nations as a benchmark for national self-assessments in areas such as energy or communications.[2] These requirements are regularly updated in the face of new developments, such as the introduction of the 5G communications standard.

Another NATO tool to respond to hybrid threats is the newly created Counter-Hybrid Support Team (CHST) concept. A CHST would consist primarily of civilian experts who could be sent at an Ally's request. A CHST could be deployed in a crisis, but given its expertise in strategic communications, counter-intelligence or the protection of critical infrastructure it can also act as an advisory team for setting up national defense structures that are better geared towards meeting hybrid threats. CHSTs are a clear sign of NATO's attempt to develop response options below the threshold of Article 5, the collective defense obligation enshrined in the Washington Treaty. That said, however, allies have also stated that hybrid attacks can trigger Article 5.

Progress has also been made in the aforementioned area of collective attribution. Strictly speaking, attribution remains a sovereign decision by each state. However, when Russian agents attempted to kill a former double agent in the British city of Salisbury in March 2018, practice went ahead of theory. Most NATO and EU member states publicly attributed the assault to Russia, and NATO allies and partner countries consequently expelled numerous Russian diplomats. Such demonstrated resolve could have a deterrent effect against at least some hybrid actors.

The multi-faceted nature of hybrid threats has also prompted NATO's political leadership to try out new meeting formats, thereby deliberately moving beyond the traditional meetings of Heads of State and Government and Foreign and Defense Ministers. In May 2019, for example, the first ever informal meeting of the North Atlantic Council with national security advisers and other senior officials took place, focusing on hybrid challenges and the need for a whole-of-government approach to meet them.

Challenges

NATO's approach to tackling hybrid threats has led to a consistent broadening of its counter-hybrid toolbox, including its relations with other actors, notably the European Union. However, there are several areas where much more needs to be done.

The Role of Military Means

First and foremost, the role of military means in deterring or defending against hybrid attacks is still not fully understood. If certain hybrid actions such as cyberattacks, "fake news"

campaigns or interference in elections are to become a permanent component of interstate competition, the role of military deterrence is likely to remain small. Military means would serve primarily to ensure that a hybrid conflict does not turn into a military conflagration. If, on the other hand, hybrid attacks were only a precursor to a military attack, as was the case in Ukraine in 2014, the defender might have to deploy his military assets earlier.[3] While it may seem unlikely that NATO would respond kinetically to a hybrid, non-kinetic attack and thus be the first to cross the threshold of using armed force, it is important that allies have a firmer grasp of the military and non-military response options. Determining when and how to respond to a hybrid campaign may well turn out to be one of NATO's toughest challenges in the years ahead. In any case, the mere assertion that more military muscle also produces more deterrence against hybrid warfare is clearly insufficient.

Cooperation with Other Actors

The logic of hybrid threats requires NATO to cooperate with other actors such as the EU and the private sector. However, this cooperation has natural limits due to different goals, memberships and working methods of these respective actors. While some political constraints can be circumvented through informal cooperation on the working level, other steps, such as the exchange of confidential information or classified documents, will remain unattainable. This makes it all the more important to develop a culture of trust between representatives of international organizations and the private sector – communities in which solutions can be discussed pragmatically and without too much "political correctness."

The Fuzzy Hybrid Debate

Perhaps the greatest challenge remains the fuzzy character of the Western hybrid debate itself.[4] This debate is characterized by the use of imprecise terminology, sweeping generalizations and much exaggeration. If, for example, a term such as "hybrid warfare" is used to describe virtually all non-military activity, even non-military strategic competition between states would become a "war." Leaving aside the problems that such an approach would pose in terms of international law, the tendency to characterize almost any unwelcome behavior as a "hybrid threat" or even a "war" generates unnecessary alarmism that makes a rational debate impossible. He who believes himself to be in a permanent state of hybrid war, or demands that NATO offer protection against every conceivable hazard, applies a perfectionist standard that no organization could ever meet. This is all the more unhelpful as the jury is still out on whether hybrid means are really as successful as some claim: even in Ukraine, Russia did not advance as smoothly as the Kremlin may have hoped initially. The "fog of war" also applies to hybrid war.

INFORMATION SERIES
Issue No. 448 | November 4, 2019

Conclusion

The defense against hybrid threats is a long-term strategic challenge for NATO, requiring profound changes in its planning and decision-making processes. In the post-Cold War era of crisis management, these processes were mostly sequential, i.e. one problem could be addressed after another. In the age of hybrid threats, a more dynamic approach is needed: Based on a continuously updated assessment of the strategic environment, options for collective action - including non-kinetic action - must be developed, exercised and, eventually, employed. For an Alliance that for decades used to focus solely on military responses to military challenges, this adaptation may be painful. However, when opponents increasingly operate in the grey zone, NATO can no longer afford to think only in black and white.

1. North Atlantic Treaty Organization, "NATO's Response to Hybrid Threats," August 2019, available at https://www.nato.int/cps/en/natohq/topics_156338.htm.
2. See Wolf-Diether Roepke and Hasit Thankey, "Resilience: the first line of defence," *NATO Review*, February 27, 2019, available at https://www.nato.int/docu/review/2019/Also-in-2019/resilience-the-first-line-of-defence/EN/index.htm.
3. This is one of the reasons why the Hybrid Strategy's categorization of NATO's response spectrum ("Prepare-Deter-Defend") does not always sit well with the military approach, which views hybrid in a less compartmentalized way and rather as a continuum between peace, crisis and war.
4. See Michael Rühle, "Deterring Hybrid Threats: The need for a more rational debate," NATO Defense College, *NDC Policy Brief* 15-2019, July 9, 2019, available at http://www.ndc.nato.int/news/news.php?icode=1335.

The National Institute for Public Policy's *Information Series* is a periodic publication focusing on contemporary strategic issues affecting U.S. foreign and defense policy. It is a forum for promoting critical thinking on the evolving international security environment and how the dynamic geostrategic landscape affects U.S. national security. Contributors are recognized experts in the field of national security.