Hybrid Warfare of the Future:

Sharpening NATO's Competitive Edge

Key Campaign Insights | July 2021

From January to July 2021, the Center for European Policy Analysis (CEPA) led a digital campaign, in partnership with the U.S. Mission to NATO, to help the transatlantic alliance imagine and creatively prepare for future hybrid threats. The campaign engaged diverse and nontraditional voices across the security, policy, and technology communities in allied and partner publics. Through a series of articles, infographics, interviews, and polls; a meme, video, and short story contest; and a culminating virtual town hall event, the initiative provided a unique forum for both next-generation and established voices to explore what hybrid warfare means, how it will evolve over the next decade, and how NATO can best counter it. Key insights from the campaign are summarized below.

THE HYBRID CHALLENGE

Hybrid warfare combines military and nonmilitary as well as covert and overt means, such as disinformation, cyberattacks, economic coercion, lawfare, corruption, and irregular and regular forces. Hybrid methods are used to blur the lines between war and peace. They attempt to undermine target institutions and populations to achieve strategic aims. While these threats are not new, technological advancements and increasing global connectivity have recently expanded their speed, intensity, and scope. To more effectively tackle future hybrid threats from Russia, China, and non-state actors, the transatlantic community and NATO should improve in the following key areas.

Raise public awareness of hybrid threats. To counter hybrid threats, the transatlantic community must first understand what they are. *Participants in the digital campaign*

The 2021 Brussels Communiqué Sufficiently Recognized the Growing Challenge that Hybrid Threats Pose for the Alliance

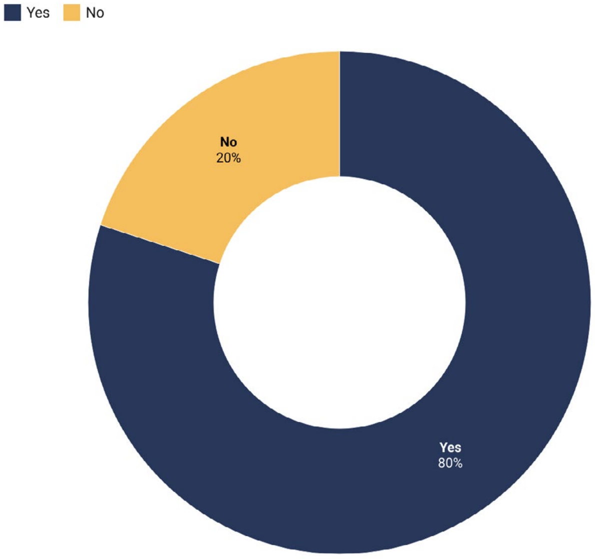

Chart: Center for European Policy Analysis • Created with Datawrapper *considered disinformation and cyberwarfare to be the most common and pressing hybrid threats of today.* On the other hand, there was less awareness of economic coercion, political subversion, and lawfare. Experts noted that while the existence of these threats is acknowledged individually, their use in conjunction makes them increasingly disruptive and their interconnectivity is underexplored. There is an urgent need to understand the impact of these threats on transatlantic societies and institutions and which hybrid actions are most likely to succeed or cause damage to allies in the future. *Future hybrid threats that require more attention include weaponized corruption, automated armies, and biowarfare.* 80% of respondents to a campaign poll believed NATO's 2021 Brussels Summit Communiqué adequately prioritized hybrid threats.

Increase NATO's speed of recognizing hybrid threats. Looking to the future, participants agreed the alliance must be able to more quickly recognize and respond to hybrid campaigns before they can fully unfold and achieve their aims. This requires investing more in intelligence, surveillance, and reconnaissance capabilities; leveraging open-source information; and utilizing human-machine teaming to compete with adversaries that have more centralized, rapid decision-making than NATO. These capabilities can aid in the attribution of hybrid actions to their perpetrators, which are purposefully difficult to detect. *To help the alliance better recognize, conceptualize, and plan for hybrid threats, campaign participants suggested NATO consider a sixth "cognitive" or "human" domain of future warfare.*

Panelists at the Hybrid Futures virtual town hall event. From left to right: Teri Schultz, Ben Hodges, August Cole, Baiba Braže. Photo: CEPA

Get comfortable operating more proactively below the threshold of conflict. Hybrid threats often fall below NATO's Article 5 threshold of armed attack laid out in its founding treaty. This makes it difficult for NATO member states to respond swiftly and appropriately in collective defense. NATO has already acknowledged that a serious cyberattack can trigger Article 5. But rather than waiting for today's ongoing cyberattacks to escalate to that level, *93% of survey respondents agreed NATO must play a more proactive role in addressing below-threshold hybrid threats.* For example, NATO could help coordinate more active and persistent cyber defense capabilities from nations, such as "hunt forward" teams. Under Article 3 of its founding treaty, NATO can also help nations mitigate the effects of hybrid threats by setting resilience standards and capability targets.

Build trust between governments, institutions, and publics. *Survey respondents overwhelmingly agreed that national governments bear the most responsibility for countering hybrid threats.* But their trust in officials and institutions to take such action varied greatly, with nearly 50% of respondents rating their trust levels at three on a five-point scale. This lack of confidence plays directly into the aims of adversaries' hybrid campaigns, inhibits societal resilience, and undermines government response. NATO ally and partner publics should engage in more civil education campaigns and trust-building exercises to strengthen democracies against hybrid threats.

Boost public-private cooperation against hybrid threats. Experts highlighted that the private sector often owns or operates much of the critical infrastructure that is targeted by hybrid warfare — from energy pipelines to electric grids to online platforms. To spot and stem future hybrid threats, a majority of participants agreed that governments, militaries, and security institutions such as NATO must work more closely with the private sector to develop indications and warning systems, response protocols, and resilience and threat mitigation measures against hybrid warfare. Governments should also engage to provide legal parameters and budgetary incentives for private sector compliance.

Innovate for tech-enabled hybrid threats. Emerging and disruptive technologies are making hybrid warfare more complex, dynamic, and formidable. To prepare for the future, NATO and its member states must invest in new technologies to strengthen their own edge against tomorrow's hybrid threats and creatively

What Technologies are Most at Risk of Being Manipulated Through Hybrid Threats?

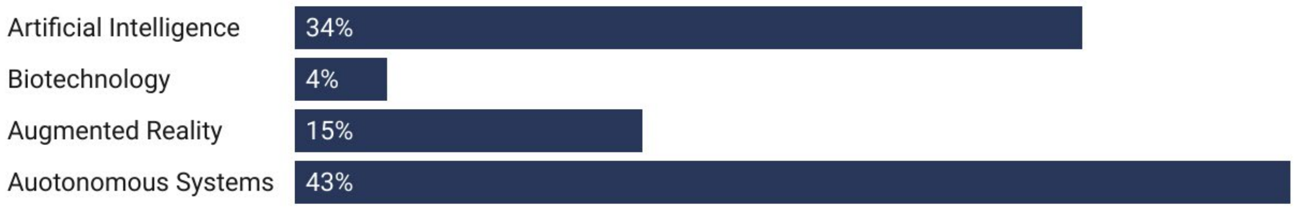

Chart: Center for European Policy Analysis • Created with Datawrapper

imagine how adversaries might use technology to exploit transatlantic vulnerabilities. *Next-generation survey respondents viewed the technologies most at risk of manipulation through future hybrid warfare as autonomous systems (43%), artificial intelligence (37%), augmented reality (15%), and biotechnology (4%). 71% also believed artificial intelligence would be the biggest game changer in the alliance's ability to counter hybrid threats in the next decade.* A majority of participants agreed NATO should play a stronger role in setting standards for the use of technologies, including in cyberspace.

Train and exercise to failure. To adequately prepare for hybrid warfare of the future, the transatlantic community and NATO must train and exercise based on complex, real-world scenarios. Experts underscored that many current institutional exercises are planned in advance and stop short of perceived limits to avoid public failure. But training to failure is a crucial way to address vulnerabilities and draw out lessons learned in preparation for future threats. More experimental, innovative counter-hybrid exercises are needed with involvement from the private sector, civil society, nations, and transatlantic institutions.

Leverage NATO as a broader forum for whole-of-society coordination against hybrid threats. Because hybrid threats are so diverse and interconnected, they fall outside the mandate of any single government department, organization, or company. This makes it difficult for nations to organize, resource, and delegate authorities to sufficiently counter them. While nearly all participants favored whole-of-society approaches to combatting hybrid threats, this is challenging to achieve in practice, especially at the transatlantic level. Some argued that NATO should serve as the wider forum to connect the military and nonmilitary personnel and capabilities required to comprehensively address hybrid threats. Building on its current efforts within the alliance, NATO could expand its information-sharing, capacity-building, exercising, and operational functions to coordinate counter-hybrid actions more robustly across nations, the private sector, and civil society. *98% of respondents believed greater cooperation with likeminded allies and partners is a more effective strategy for tackling hybrid threats than isolationism.*

UNITED STATES MISSION
NORTH ATLANTIC TREATY ORGANIZATION

This project was funded by a grant from the United States Department of State. The opinions, findings and conclusions stated herein are those of the authors and do not necessarily reflect those of the United States Department of State.