zif Center for International Peace Operations

100 Voices on Technology & Peace Operations

Managing cyber security in peace operations

How NATO Can Respond to Hybrid Challenges

18 November 2021 | Michael Rühle

Traditional notions of military security used to be state-centric and focused on the defence of borders and territory against an aggression by another state. Today, such scenarios are increasingly giving way to a complex mix of military and non-military threats that can also affect societies from within. Through cyberattacks or social media campaigns, adversaries seek to destabilise entire societies without a single soldier crossing a single border. And the "hybrid" combination of military and non-military tools creates ambiguity that makes decision-taking by consensus much harder.

NATO is based on traditional notions of deterrence and defence against armed attack. Its founding treaty even defines the specific territory that is eligible for collective protection. Unsurprisingly, the emergence of "de-territorialised" hybrid threats poses a considerable challenge for the Atlantic Alliance. The answer does not lie in more tanks or missiles, but in a new toolbox that seeks to provide networked responses.

TEN RECOMMENDATIONS

First, improve situational awareness. Allies must be able to "connect the dots", i.e., to recognise a hybrid campaign early on. To this end, Allies have expanded their intelligence cooperation within NATO. Moreover, NATO is expanding its own strategic analysis capabilities, which allow for a more forward-looking and sometimes more provocative open-source approach toward emerging challenges. Accordingly, the scope of analysis ranges from the security implications of Artificial Intelligence to the strategic consequences of the Bitcoin cryptocurrency.

Second, enhance training and education. The growing importance of non-traditional challenges makes them a permanent fixture in NATO's education and training programmes. Diplomats and military leaders alike must be given the opportunity to develop a better understanding of how cyberattacks, energy cut-offs or disinformation campaigns determine future conflicts. To this end, NATO has set up dedicated courses at its training facilities as well as at its various Centres of Excellence.

100 Voices on Technology & Peace Operations

Third, adapt exercises. Today, even a "traditional" military conflict would include numerous cyber elements, the targeting of energy and other critical infrastructure, and massive disinformation campaigns. It is largely through exercises that one can understand the effects of these non-traditional threats. The integration of hybrid challenges in NATO's exercises reflects an awareness of this fact. This is also important for enhancing the resilience of partner countries. For example, NATO and Ukraine conducted several table-top exercises on strengthening the resilience of Ukraine's electricity network.

Fourth, enhance resilience. Assuming that certain types of attacks, such as cyber or hybrid attacks, cannot always be deterred, the focus of the defender needs to shift toward resilience, i.e., the ability to take the hit, minimise its consequences, and bounce back. Resilience measures, such as the protection of critical cyber or energy infrastructure, are largely a national responsibility. However, NATO can assist nations in conducting self-assessments that help identify vulnerabilities.

Fifth, exchange best practices among Allies and with partner countries. Ukraine and Georgia can offer valuable experience on Russia's hybrid tactics. Australia can offer experience on China's political influence campaigns. Israel can contribute its experience in dealing with non-state actors. Allies and partners also need to exchange experience on new legislative tools they employ against hybrid actors – for example withdrawing broadcasting licenses from "fake news" media outlets, or not allowing certain countries to buy strategically critical companies. Over time, this should lead to a repository of experience that will help countries in meeting hybrid threats.

Sixth, develop links with other international organizations. The nature of non-traditional security challenges makes NATO's success increasingly dependent on how well it cooperates with others. Consequently, NATO must be connected much better to the broader international community. This is particularly true for its relations with other security stakeholders such as the European Union and the United Nations, who have certain legislative powers against hybrid aggression that NATO lacks. It is also true with respect to nongovernmental organizations and think tanks, where much untapped expertise resides.

Seventh, develop links with the private sector. With most energy and cyber networks in private hands, it will be crucial to build public-private partnerships. The goal should be to establish "communities of trust" in which different stakeholders can share confidential information on cyberattacks and other security concerns. This will be challenging, since national business interests and collective security interests may sometimes prove to be irreconcilable. Still, the nature of many emerging security challenges makes the established compartmentalization of responsibilities between the public and private sectors appear increasingly anachronistic.

Eighth, improve collective decision taking. Given the ambiguity of many hybrid actions, it is essential that the Allies rapidly achieve a common understanding of the threat but also on the response. In some cases, such as cyberattacks or fake news campaigns, the slow, deliberative nature of consensus building in NATO could prove unsuitable for the challenge. Sometimes the consensus on a response must be built before the attack occurs. Hence, nations will need to have

certain rules of engagement already in place, or pre-delegate authority to certain entities. Exercises – especially those that involve high-level decision-makers – are a major tool for highlighting potential deficiencies in decision taking.

Ninth, understand Emerging Disruptive Technologies. "Big data" analysis, autonomy, or block chain technologies may offer huge security benefits. Artificial Intelligence, for example, can help to detect "fake news" campaigns on social media. However, such technologies can also empower adversaries to orchestrate smarter and stealthier hybrid attacks. Hence, understanding the security (and moral) implications of new technologies is a precondition for understanding the future of hybrid conflict. At the same time, NATO should have a voice in the search for new norms of acceptable behaviour in new domains, such as space, and in new "virtual" domains, such as cyberspace.

Tenth and finally, create new tools to meet non-traditional challenges. Counter Hybrid Support Teams that offer tailored technical or political advice can increase a vulnerable Ally's resilience. Collective attribution might deter certain hybrid aggressors from going too far, in particular if coupled with some forms of punishment (e.g., the expulsion of diplomats, sanctions). Best-practice exchanges on how to deal with hostile influence campaigns, or on how best to organise the protection of critical energy infrastructure, can increase Allies' and partner countries' collective IQ in meeting these challenges.

CONCLUSION

Largely due to technological developments such as cyber and social media, hybrid activities have become a constant feature of international relations. Yet there is no law of nature that would make this unpleasant situation inevitable or permanent. Most hybrid actors have a face and an address. They can be countered, punished, sometimes deterred, but they can also be engaged. Western unity is key. If the West stays united, refuses to accept hybrid conflict as the "new normal", and learns how to get better at meeting threats in the "grey area", it can blunt the hybrid weapon even if it may never completely eradicate it.

ABOUT THE AUTHOR

Michael Rühle is Head, Hybrid Challenges and Energy Security Section in NATO's Emerging Security Challenges Division. The views expressed are the authors' own.