Hybrid CoE
The European Centre of Excellence for Countering Hybrid Threats

StratByrd CONSULTING

Jointly organized by Hybrid CoE, Community of Interest Strategy and Defence (COI S&D) and StratByrd Consulting

TEASER

Hybrid Warfare: Future & Technologies (HYFUTEC)

Mind the gaps

R. Thiele/J. Schmid

New technologies have a catalytic effect on hybrid methods and tools. They improve the starting conditions for hybrid action, expand the arsenal of hybrid players and thus help to increase the reach of their activities as well as their prospects of success. At the same time, new technological developments may offer options to better identify, understand, defend against and counter hybrid attacks. In order to prevent, deter and – if necessary – outmanoeuvre hybrid opponents, it is therefore important for political, civilian and military leaders and decision-makers, as well as for industry and academia, to develop a common and comprehensive understanding of the implications of new technologies in a hybrid warfare/conflict context.

With this in mind, the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE), and its Community of Interest on Strategy and Defence (COI S&D) have initiated the Hybrid Warfare: Future & Technologies (HYFUTEC) project, aimed at assessing and enhancing understanding of the disruptive potential of new technologies in the context of hybrid warfare/conflict. The project was launched in March 2019 with a series of events (in Helsinki, Berlin, Vienna, and Stockholm). An online educational event (HYFUTEC curriculum) was provided for the Baltic Defence College (Tartu). Within its broad future & technology horizon scanning, the project has identified 19 technological trends with urgent and profound implications in the context of hybrid scenarios.

The project findings point to hybrid actors that have exploited the current conceptual and resulting capability gaps of the West. Several of these actors are making skilful use of inexpensive, commercially available technologies to further their own ambitions and power objectives. This development opens the floodgates to coercion and blackmailing by malicious actors, thus putting NATO and EU cohesion and solidarity at risk.

HYFUTEC 19 comprises the 19 technologies that this study has identified as particularly relevant for the evolution of hybrid challenges, conflict and warfare, namely: 5G; additive manufacturing; artificial intelligence; autonomous systems; biotechnology; cloud computing; communication networks; cyber and electronic warfare; distributed ledger; directed energy; extended reality; hypersonics; the internet of things; microelectronics; nano-materials; nuclear modernization; quantum sciences; space assets; and ubiquitous sensors. These emerging technologies are likely to drive developments in hybrid conflict/warfare in the coming years. Seven of these technologies would appear to have a prominent role and have been examined in more depth: **5G; artificial intelligence; autonomous systems; cyber and electronic warfare; extended reality; quantum sciences; and space.**

A technologically smarter and connected world affects how wars will be fought in the future. The extremely dynamic, ongoing technology race is driving cross-domain networking and the virtualization of functions in armed forces and societies. It combines virtual worlds and reality, and private and professional life with each other. Combining the possibilities of new technologies and the further development of operational concepts has been key to the successful Russian and Chinese rise in military capabilities across all operational domains – space, cyber, air, sea and land – and lies at the very core of their excellence in hybrid warfare. They have developed capabilities in the field of anti-access and area denial (A2/AD), such as ballistic and cruise missiles, offensive cyber weapons, and electronic warfare. They have not only become military, but also technological rivals of the West – and are beginning to gain an edge.

Digitalization is the price of admission to participate competently and self-determinedly in economic and social networks today. It is also, increasingly, a core issue of security and defence policy. The capacity to own – and the ability to access, organize, interpret, and distribute – data are at the very core of digitalization. In a world of constant connectivity, data is the new oil and networks are the new oil rigs. Consequently, data needs to be refined to deliver actionable information. New smart and digital technologies facilitate finding and tracking this data and make its inherent information actionable. This provides new opportunities in a positive sense, but at the same time opens up a broad spectrum of potential hybrid attack vectors. In the recent past, actors such as Russia and China have repeatedly demonstrated that physical presence is no longer needed to achieve considerable tactical, operational and even politico-strategic objectives with relatively low risk of attribution and low use of resources.

Driven by the catalytic effect of new technologies, hybrid warfare can be expected to become a long-term strategic challenge. It is therefore paramount to develop a comprehensive understanding of the impact of new technologies in a hybrid warfare/conflict context.