

Mateusz Rakowski

Hybridity and asymmetry of future wars in cyberspace

Doctoral dissertation in the discipline of political and administrative sciences written under the scientific supervision of dr. hab. Andrzej Dubicki, prof. at the University of Lodz

Abstract

The doctoral dissertation analyses the transformation of contemporary conflicts under the conditions of the digital revolution, with particular emphasis on the role of cyberspace in shaping their asymmetric, irregular, and hybrid character. The starting point of this study is the assumption that war, as a historically variable phenomenon, remains closely linked to technological development. It is further assumed that digitalization has produced a qualitative transformation of the battlespace, in which information, infrastructure, and operations have become durably intertwined.

The objective of the dissertation is a critical examination of the concept of “new wars” and an assessment of how cyberspace influences the dynamics of present and future conflicts. This study focuses on the concepts of hybridity and asymmetry, exploring their historical development and contemporary application within the network-centric environment. The study addresses the validity of dominant conceptual categories, especially the notion of hybrid warfare, the role of cyberspace as a domain of operations, and the limits of their analytical usefulness under conditions of increasing complexity and uncertainty.

The central research hypothesis is that cyberspace does not function as an autonomous domain of conflict; rather, it structurally permeates other domains of action, thereby reinforcing asymmetry, irregularity, and hybridity. Consequently, conflict is not merely “transferred” into cyberspace. Instead, it exploits its functional characteristics, namely the low barriers to entry, the attribution difficulties, the cascading effects, and the absence of clearly defined geographical boundaries. These measures have the effect of lowering the threshold for the initiation of hostilities, thus enabling an escalation in the level of involvement on the part of non-state actors.

Methodologically, the dissertation is grounded in systems analysis, complemented by an interpretative approach as well as comparative and historical analysis. This framework facilitates the comparison of Western, Russian, and Chinese theoretical and doctrinal perspectives, in ad-

dition to a critical examination of concepts such as the Revolution in Military Affairs, hybrid warfare, and waves of conflict development. The empirical basis consists of strategic and doctrinal documents and analyses produced by state institutions and the private sector, supplemented by case studies of conflicts in which cyber operations have played a significant role.

The findings demonstrate that asymmetry and hybridity are historically persistent features of conflict. However, digitalization has radically altered their scale, tempo, and multi-layered character. Cyberspace has become an environment of constant strategic pressure, in which the boundary between peace and conflict is increasingly blurred. Concurrently, the analysis demonstrates that states, in response to the escalating vulnerability of critical infrastructure, seek to enhance resilience through partial de-digitalisation, system isolation, and the design of disruption-resistant solutions. Nevertheless, the study demonstrates that full de-digitalisation at the strategic level is not feasible due to the structural dependence of economies, logistics and innovation on the digital environment.

The dissertation's key conclusion is that a paradigm of permanent uncertainty must be adopted in the analysis of contemporary conflicts. This uncertainty is of an epistemic, ontological, operational and strategic nature, and prevailing concepts of hybrid and asymmetric warfare prove insufficient insofar as they remain rooted in categories derived from kinetic conflict. In response, the dissertation proposes a probabilistic, recursive risk-assessment model applicable at the strategic, operational and tactical levels. The purpose of the model is not to predict specific scenarios, but rather to ensure that decision-making remains stable in conditions of persistent—or even permanent—uncertainty.

The dissertation concludes that future conflicts will be characterised by enduring domain interpenetration, increasing asymmetry, and the growing centrality of resilience as a key element of strategic advantage. Cyberspace does not constitute an alternative to kinetic violence. Instead, it has been shown to facilitate its brutalisation and to deepen processes of dehumanisation, both within the digital sphere and beyond it.

Keywords

Hybrid Warfare, Asymmetric Warfare, Future Warfare, New Wars, Gibrinaya Voyna, Zhinenghua Zhanzheng, Cyberspace, Digital Resilience.