Hybrid and Cyber War as Consequences of the Asymmetry

A Comprehensive Approach Answering Hybrid Actors and Activities in Cyberspace. Political, Social and Military Responses

Bearbeitet von
Dieter Muhr, Bahram M. Rajaee, Josef Schröfl

ISBN 978 3 631 60285 0
Format (B x L): 14 x 21 cm
Gewicht: 500 g
Introduction

Over the past few years, the editors of *Hybrid and Cyber War as consequences of the Asymmetry* have focused on the subject of asymmetry as a political phenomenon in contemporary security affairs. While this emphasis has been on the humanistic and social dimensions, due to the multifaceted nature of the subject matter, the research presented here is interdisciplinary as well as largely political-military in scope.

In the first book of this series, published in 2004, the subject was examined with regard to its theoretical underpinnings, significance as a phenomenon characterizing the new face of war, impact on international relations and world politics, and the attendant ethical and military implications. The continuation of our research agenda - in the form of a second book published in 2006 - focused on selected aspects of asymmetry on the national and international levels. This book related the subject to themes such as western society, the monopoly of power by the nation-state, state-building, pre-emption in asymmetric conflicts, economics, conflict communication, child soldiers, and political violence and terrorism.

This foundation, and the ensuing third and fourth projects, established a baseline for the preceding volume that was published in 2009 and entitled *Winning the Asymmetric War*. This book discussed both the causes and effects of asymmetrical patterns in a globalized world and demonstrated once again that the complex reality of asymmetrical threats can only be addressed when all relevant political, social, and crucial cultural dimensions are accounted for when formulating national and international security strategies.

In recent years, two essential and rather new ingredients for asymmetric warfare emerged: hybrid actors and activity in cyberspace. Hybrid orders and actors emerge in environments where elements of both conventional and unconventional warfare coexist - and the extension of the battlespace to the cyber domain has provided a entirely new theatre where hybrid war can be waged. Thus, these new factors have produced an even greater increase in the level of complexity inherent in asymmetric war. For this reason, more comprehensive approaches to the challenge of asymmetric warfare are required today.

---

1 Schröfl/Pankratz (Edt.): “Asymmetrische Kriegführung – ein neues Phänomen der internationalen Politik”, NOMOS, Frankfurt/Germany.
2 Schröfl/Pankratz/Micewski (Edt.): „Aspekte der Asymmetrie – Reflexionen über ein gesellschafts- und sicherheitspolitisches Phänomen“, NOMOS, Frankfurt/Germany.
The asymmetrical configuration of international relations, as well as responses to it in terms of strategies to protect populations and prevent conflict, demand an understanding of the interdependent variables that shape asymmetrical threats. In turn, these factors are grounded in the political and societal structures and processes of individual, national, and international relations as they emerge in their respective cultural settings and environments.

Afghanistan, for example, has recently become a synonym for not only a failed state but also for current missions and their challenges and risks. It is the leading, but not the only, example of what missions and crisis management in the 21st century are all about. Crisis management has become one of the key civil and military activities that states engage in; moreover, such operations have been transformed considerably in the past decade. Missions/operations in the 21st century may take on a variety of characteristics and forms that will combine military and civilian elements. They can also evolve significantly during the period of a mission or operation - and sometimes do so in dramatically different directions.

Notably, the recent political changes in several key Arab states at the beginning of 2011 - the “Jasmine Revolution” - also highlight how asymmetries can become the leading factor for changes in political systems and how new types of warfare (such as cyber warfare) can influence developments.

Complexity is a reality, but can be overcome. Doing so requires a deeper analysis (i.e., thinking dynamically and in non-linear terms, building in feedback loops, accounting for time lags, etc.) in order to understand overt and hidden factors that are driving fundamental relationships in a particular environment, appreciate the full spectrum of actors, and effectively prepare for extant and emerging challenges. Intervening in such “hybrid orders” with traditional tools such as so-called “surgical interventions” or conventional approaches to warfare will not alter the hybridity of actors and the environment in which they operate. Actions such as retaliation in a traditional sense can in fact yield unanticipated outcomes in hybrid environments, without allowing for the chance to assess the outcome. This situation has intensified because local actors can now compensate for their conventional inferiority vis à vis external intervening forces via new dimensions of asymmetrical warfare, such as cyber war or through the Internet.

Thus, the combination of Cyber Warfare and Hybrid Warfare represents an explosive blend of factors that has enabled adversaries to leverage their relatively meager resources. For Western strategists and decision makers, this means that the apparently and traditionally weaker part of the adversarial equation has now received additional advantages and opportunities through the asymmetry of modern warfare.

An appropriate Comprehensive Approach must encompass very robust interfaces across all relevant dimensions of response planning. Robustness is required in that the application of a Comprehensive Approach very often is not
in the direct or obvious interest of states intervening in hybrid orders, and in many instances this weakness has hindered effectiveness. Strengthening linkages - conceptual, institutional, and operational - between and among the essential domestic and international ingredients for implementing a Comprehensive Approach is a prerequisite for success.

As the environments of hybrid orders are inherently complex and dynamic, it is also not beneficial to employ static strategies and goals, via static means and approaches. Although a strategy can be defined as a product of a compromise by participants in a Coalition, it needs to be comprehensive as well to support the necessary opportunities for that Coalition.

The successful application of a Comprehensive Approach therefore requires a flexible and adaptive strategy and vision. For this reason, on-going reflection on all these elements is also an indispensable prerequisite for an effective response.

Thus, the core theme of this new volume, the sixth of the series, is to identify the problems caused by hybridity and Cyber War given the broader nature of Asymmetry and Asymmetric Warfare. In addition, those broader challenges will themselves be further analysed in various contexts. Moreover, interactions between these themes and key actors will be described and trajectories for possible solutions will also be offered.

We hope that our distinguished readers will find an informative basis for better appreciating the new, highly combustible mixture of Hybrid War and Cyber War, in the context of Asymmetry and Asymmetric Warfare at the beginning of the 21st century.

Schroefl / Rajaee / Muhr