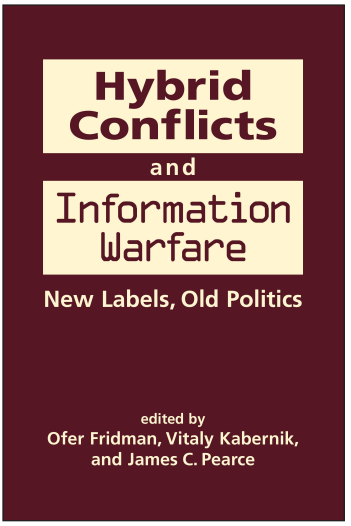
EXCERPTED FROM

# Hybrid Conflicts and Information Warfare: New Labels, Old Politics




edited by
Ofer Fridman,
Vitaly Kabernik,
and James C. Pearce


ISBN: 978-1-62637-751-6 hc

LYNNE RIENNER PUBLISHERS

1800 30th Street, Suite 314
Boulder, CO 80301 USA
telephone 303.444.6684
fax 303.444.0824

# Contents

# 1

# Hybrid Conflicts and Information Warfare

*Ofer Fridman, Vitaly Kabernik, and James C. Pearce*

**Two significant events marked the year 2014 as a turning** point in the history of international security: the Russian involvement in the Ukrainian crisis and the rise of the Islamic State in Syria and Iraq. The most focal characteristic, which these two independently evolved confrontations share, is not necessarily the relative success of political actors (either Russia or the Islamic State) in achieving their territorial gains, but rather their successful use of informational space by an effective employment of novel communication capabilities. The Information Revolution that had been occurring for the past two decades has finally manifested itself in the way that political players conduct, interpret, and perceive conflicts. The concept of *hybrid warfare* was one of the first attempts of the expert community to address this rapidly changing character of conflicts, where a smart employment of newly available technologies to influence the hearts and minds of targeted audiences offers significantly better results than any real actions.

It is important to note that there was little novelty in the idea itself, as disinformation campaigns, propaganda, and other attempts to use informational space for political goals have been around for thousands of years. However, while the manipulation of information successfully executed by an adversary is a virus, as old as politics itself, today's information technologies allow this virus to be disseminated much further and much faster than ever before. It does not necessarily mean that the virus is stronger or the victims are weaker. It simply means that more people are exposed—and this alone offers a huge advantage to anybody who attempts to influence hearts and minds in the post–Information Revolution era of the early twenty-first century.

The technological and informational revolutions of the past two decades have amplified the danger posed by nonmilitary means and methods of political struggle, in general, and in the information dimension in particular. While the Western world is preoccupied by the Kremlin's alleged interference in the US presidential elections in 2016 or Russia's other alleged attempts to subvert and destabilize the Western democracies by successful information operations, Russian decisionmakers are notably anxious about Western attempts to manipulate Russian information against the current government. Moreover, the rapid success of the Islamic State in recruiting thousands of young people across the world surprised both Russia and the West, demonstrating the new dangers of the manipulated flow of information multiplied by modern communication technologies.

In light of these developments, three main issues have been occupying the academic and professional discourse in regard to contemporary conflicts. The first one has been the idea of increasing hybridity between different military and nonmilitary means and methods employed by political players to achieve their goals without escalating to an outright open armed confrontation. The second one has been the increasing role of the informational dimension as a virtual space, used to promote certain political goals, either domestically or internationally, or both. The third major topic has been the rise of the Islamic State with a whole set of problems and threats that it brought to international security and stability. While it seems that the core territorial base of the Islamic State has been destroyed, it is difficult to conclude the same about its ideology and its influence spread through the modern communication technologies. Moreover, as several chapters of this book point out, there are much bigger geopolitical problems that allow to the ideology of the Islamic State to flourish, and the main lessons that the rest of the world should learn rest not in the tactics of counterinsurgency but in the field of strategic communications.

In analyzing the parallel discourses that have developed in the West and Russia on these three topics, it is possible to point to two main narratives. While discussing the role of hybridity and the information dimension in international relations, both Russian and Western scholars and experts swiftly fall into the field of mutual accusations. Their conceptual understandings of the hybrid environment, as well as the importance of influence and control of information for achieving political goals, are starkly similar. Moreover, when it comes to analyzing the hybrid activity of the Islamic State, or the way it exploits the information dimensions, it seems that Russian and Western opinions share even more similarities than differences.

This book brings, for the first time, both Russian and Western scholars to discuss the most sensitive and timely topics such as the role and nature of hybridity, information warfare, and strategic communications in contemporary world politics. The unique academic collaboration presented in this book takes place at a challenging time in international relations, as a confluence of conflict-related insecurities has given rise to a sense of deep crisis. Closely associated with this are concerns relating to the increasing use of propaganda, espionage, subversion, and cyberattacks by state and nonstate actors. Such concerns have recently taken a prominent role in the contemporary international public discourse. The current political climate presents challenges to the free academic exchange of views and opinions, yet also renders it of critical importance. This book offers a dialogue on pressing issues relating to international order, peace and security, and building bridges between societies by fostering and supporting the development of a more inclusive international public discourse.

The book consists of three main conceptually interconnected parts. Each section includes two chapters written by Russian scholars and two written by Western scholars. One of the most important rationales of the book is that these chapters are not structured as one versus the other, but to represent a dialogue of opinions. In other words, the purpose is not to contrast the Russian and the Western views on hybridity, strategic communications, or the Islamic State's propaganda, but rather to offer one integrated discourse that benefits from both Eastern and Western perspectives on conflicts in the twenty-first century.

After this brief introduction, Part 1 of the book focuses on the idea of hybridity in contemporary conflicts. In the opening chapter, David Betz discusses the development of the idea of hybridity in Western military thought, its advantages and weaknesses, as well as the main contribution of the concept of the so-called hybrid war to the Western political-military debate and decisionmaking processes. While the concept has been widely discussed in the existent literature,[1] Chapter 2 offers a fresh perspective by analyzing the Russo-Japanese War and arguing that the concept of *hybrid war* is simply an answer to contemporary erroneous expectations for wars to be easy, cheap, and decisive.

This insight into the Western understanding of hybridity is followed by Chapters 3 and 4 by Georgy Filimonov and Vitaly Kabernik, respectively. While the first sheds light on the Russian interpretation of "color revolution" in the context of hybrid war and points to the conceptual differences between the Western and the Russian approaches to hybridity, the second offers an in-depth historical-conceptual analysis of the

Russian approach through the prism of Russian traditional military thinking. These two chapters come to bridge an important gap in the currently available literature in English on the Russian understanding of hybridity. Since 2014, many Western scholars have tried to analyze Russian actions through the Western prism of hybrid war; however, the amount of research conducted to analyze the Russian perspective has been limited.[2] Chapters 3 and 4 fill this important lacuna.

The final contribution in Part 1, Chapter 5 by Ofer Fridman, compares the Russian and the Western perspectives on hybridity, making an attempt to answer one of the most important questions regarding this debate: Is hybrid war something new, in either the Western or the Russian interpretations, or is it just a new title used for the politicization of very old elements of political confrontation?

Part 2 of this book focuses on the role of strategic communications and information warfare. It opens with Chapter 6 by Mervyn Frost and Nicholas Michelsen, who discuss the ethical dimensions of informational confrontations. The world has become envisioned as beset by irreconcilable clashes of interpretations. In the turbulent information space of the twenty-first century, people have become less deferential, more questioning, and—thanks to social media—have access to too many opinions, some of which might intentionally distort the truth. One notable concern is that the criteria for identification of one's international political and military opponents widen to include anyone who threatens an actor's command of the informational space. Amid rising geopolitical tensions and public anxiety associated with campaigns by hostile state and nonstate actors seeking to shape public opinion and attitudes in pursuit of their own strategic objectives, the chapter seeks to shed light on the unavoidable ethical dimensions that arise in this information war. It aims to elucidate the ethical dimensions of acts of strategic communication, within which are included those acts referred to as *information war* by reference to the global practices within which they take place.

This general introduction to the topic is followed by a dialogue between Matthew Armstrong and Radomir Bolgov, who discuss the relations between politics and information warfare, the former presenting the case of the United States in Chapter 7 and the latter the case of Russia in Chapter 8. In his chapter, Armstrong traces the political history of the United States Information Agency (USIA)—the agency established during the Cold War to centralize and coordinate the battlefield of the minds and wills of the public on both sides of the iron curtain. Analyzing the internal politics that surrounded the establishment and the activity of the USIA, Armstrong argues that the United States never properly armed

itself for the reality of the information warfare it was embroiled in, neither during the Cold War nor after it (when the agency was abolished in 1999). Therefore, Armstrong's argument goes, in the turbulent information environment of the twenty-first century with many players who attempt to subvert US stability and interests through informational space, the United States lacks a historical precedent to draw on.

In the chapter that follows Armstrong's, Bolgov underlines the complexity of discourse and the nexus of different ideas in Russian professional and scholarly publications on information warfare. While some Western scholars claim to crack the so-called Russian information warfare,[3] Bolgov argues that in Russia itself the understanding of what this type of confrontation should (or should not) be is full of contradictions fed by different political and ideological factors. He provides an overview of the approaches to information warfare in the Russian political and expert community, including an analysis of the legal and doctrinal framework of information warfare policy in Russia. For the first time, Bolgov combines political, ideological, and theoretical factors involved in the Russian conceptualization of information warfare as well as the practical activity of actors in charge of related policies in Russia.

In Chapter 9, which closes Part 2, Oxana Timofeyeva takes Bolgov's arguments further, elaborating on the conceptual understanding of the information dimension in contemporary conflicts and on the Russian interpretation of this phenomenon. The biggest problem surrounding the discourse about information warfare in Russia, according to Timofeyeva, is a variety of different actors (military, politics, media, etc.) that attempt to manipulate the concept to suit their own agendas. After examining several recent cases of information-psychological operations conducted in the Russian media space, Timofeyeva discusses and criticizes a controversial tool created in the political environment of information warfare by the Russian Institute for Strategic Studies for monitoring the level of anti-Russian narratives in the media publications of different countries.

Based on the conceptual foundations created in the first two parts of this book, Part 3 analyzes the case of the Islamic State and its success to utilize the informational domain for a variety of goals. While Charlie Winter's in-depth analysis in Chapter 10 of the propaganda campaign launched by the Islamic State during the battle for Mosul mainly focuses on its domestic aspects, in Chapter 11 Vladimir Sotnikov discusses the implications of the successful strategic communications of the Islamic State for global security and stability. Since Winter examines in detail the information operations conducted by the Islamic State

on a tactical and operational level, and Sotnikov presents the strategic framework of the organization's actions, these two chapters uniquely complement each other by presenting for the first time the full picture of its information warfare.

In Chapter 12, Akhmet Yarlykapov examines the effectiveness of the Islamic State's propaganda in the North Caucasus. Basing his analysis on sociological and anthropological research and surveys, he points to different propaganda methods used by the Islamic State to recruit new fighters and their astonishing level of success.

In the closing chapter of Part 3 (Chapter 13), Craig Whiteside draws a conceptual line between all previously discussed topics. He argues that regardless of the title—whether it is hybrid, information, or political warfare—the contemporary conflict has become a multimodal affair with a great emphasis on the information domain, and the case of the Islamic State is a good illustration of this phenomenon.

In the concluding chapter of the book, Chapter 14, James C. Pearce makes an attempt to connect between conceptual debates and practical examples presented in the book. He ultimately comes to a conclusion that although the labels used to describe events change, there is little novelty in the politics that shape and direct them.

## Notes

1. For example, Timothy McCulloh and Richard Johnson, *Hybrid Warfare* (Tampa: MacDill Air Force Base, Joint Special Operations University Press, 2013); Frank Hoffman, *Conflict in the Twenty-First Century: The Rise of Hybrid Warfare* (Arlington, VA: Potomac Institute for Policy Studies, 2007); Williamson Murray and Peter Mansoor, eds., *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present* (Cambridge: Cambridge University Press, 2012).

2. For example, Andrew Korybko, *Hybrid Wars: The Indirect Adaptive Approach to Regime Change* (Moscow: RUDN University, 2015); Ofer Fridman, *Russian "Hybrid Warfare": Resurgence and Politicisation* (London: Hurst, 2018).

3. For example, Keir Giles, *Handbook of Russian Information Warfare* (Rome: NATO Defense College, 2016); Rod Thornton, "The Changing Nature of Modern Warfare; Responding to Russian Information Warfare," *RUSI Journal* 160, no. 4 (2015): 40–48; Jolanta Darczewska, "The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study," Point of View No. 42 (Warsaw: Centre for Eastern Studies, 2014); Keir Giles, "The Next Phase of Russian Information Warfare" (Riga, Latvia: NATO Strategic Communications Centre of Excellence, 2016); Mark Galeotti, *Hybrid War or Gibridnaya Voina? Getting Russia's Non-Linear Military Challenge Right* (Prague: Mayak Intelligence, 2016).