21 June 2024

IW PERSPECTIVES

Hybrid Warfare is Less Than Warfare: *A dangerous Illusion*

Prof. Alina Bârgăoanu and Dr. Elena Negrea-Busuioc

“Hybrid warfare”, “information warfare,” “cyber war” are popular buzzwords or catch-all phrases frequently used in the international discourse, especially in the aftermath of Russia’s full-scale military invasion of Ukraine that began in February 2022 and continues to this day. However, despite the hype, neither scholars nor practitioners have agreed on a consensus definition of the hybrid warfare phenomenon, in particular, that would add substance to the debate over the informational and public opinion dimensions of contemporary conflicts, diplomacy, and security issues.

This essay seeks to shed some light on two prevailing paradigms in theoretical treatment of hybrid warfare. Clear analysis of these two approaches will enhance reflection on society’s systemic vulnerabilities, and have practical consequences on planning and delivering adequate responses. This essay is premised on an understanding of hybrid warfare as a new type of warfare, waged with novel weapons made possible by the hyper-connectivity of the information space, as described by Mark Leonard in his book *The Age of Unpeace: How Connectivity Causes Conflict*. This new type of warfare lies at the hazy intersection between war and peace, and its “battlefield” is constituted both by formal governance processes, and by public perceptions of the legitimacy and relevance of these processes. In this battlefield, both weapons and their intended targets are non-military in nature, and thus appear to be “soft.” However, this does not necessarily make hybrid warfare a lesser, softer form of warfare in terms of its real-world consequences, which is the most consequential error in both understanding and countering it.

Two prevailing paradigms of hybrid warfare

According to the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, hybrid warfare refers "to coordinated and synchronized actions that deliberately aim at systemic vulnerabilities of democratic states and institutions, via a combination of political, economic, military, civil and information tools." As shown by the Centre's 2021 report entitled *The Landscape of Hybrid Threats*, these actions are, arguably, difficult to attribute to a particular entity (e.g., a specific military or non-military organization, government, etc.). They are also hard to detect, and they exploit the sometimes vague distinctions between war and peace. Furthermore, the same report shows that hybrid actions are characterized by ambiguity. The actors involved in such actions operate in a twilight, "grey" zone of political and military conflict, blurring well-known dichotomies between friend/enemy, legal/illegal, war/peace, state/non-state, hard/soft power, and overt/covert operations. This ambiguity is generated by a combination of conventional and unconventional means, such as disinformation, political influence, electoral interference, attacks on critical infrastructure, cyberattacks, various forms of cultural or religious influence, unlawful activities and, in some cases, the asymmetric, low-intensity use of military power.

In an article published in *Eurozine*, Mark Galeotti argued that two prevailing paradigms structure the theoretical debate on the concept of hybrid warfare. According to the first paradigm, the actions that define hybrid warfare precede, facilitate, prepare traditional military interventions. Thus, it could be said that, within certain limits, hybrid war is as old as conventional war itself: war is ... hybrid, hence, the term "hybrid warfare" is almost tautological in nature. Since the beginning of time, albeit in more rudimentary forms, any organized military invasion, by definition, is planned with consideration given to psychological and informational factors, having taken into account knowledge, exploitation, and exacerbation of the opponent's systemic weaknesses and vulnerabilities.

Galeotti's second paradigm—which we consider more in line with modern technological, social and geopolitical realities—posits that the goal of hybrid warfare is not to lay ground to a conventional military invasion; in fact, actions pertaining to hybrid war are not necessarily followed by a fully-fledged military intervention. According to this latter view, hybrid warfare is an instance of "political war," encompassing aims to be achieved exclusively through non-military, non-kinetic actions. This type of political war, which uses non-military tools to neutralize civilian and military targets alike, does not portend an invasion, but it aims to undermine, to demoralize, to divide, and to distract an opponent so that an actual military intervention becomes unnecessary and irrelevant. Put differently, hybrid war is a generalized attack on the economic, political and social fabric of a country, seeking to paralyse both government elites and public opinion from being able to take action on critical strategic issues, as shown in a recent paper on hybrid warfare and societal resilience. The governance process, including both specific policies and political system writ large, becomes the new battlefield (hence the notion of political war), while the novel "weapons" deployed are people's perceptions, opinions and sentiments, the frames and narratives structuring public conversation, the strength of the social contract between the citizen and the state, as well as the level of social cohesion and of public trust.

Irrespective of whether one considers that hybrid warfare excludes kinetic action or not, disinformation–understood as a strategic enterprise to alter the "epistemic integrity" of a society, to blur the distinction between what is real and what is not real (be it false, misleading, or synthetic)–plays a crucial role. Disinformation reduces the distinction between truth and falsehood, between facts and pseudo-facts to nothing but blurred lines: everybody gets their own version of facts, thus rendering objective, reality-based discourse almost impossible. Disinformation is a strategic enterprise to distort policy and mislead people in the target society, is aimed at both military and non-military targets, and is not an *ad hoc* manipulation of the (mainstream and social) media ecosystem for limited tactical, short-term gains. Moreover, its goal is not to persuade the target society of an arguably higher, superior political (or economic) model. Rather, it seeks to: 1) undermine decision-making processes (by postponing, delaying, blocking, or disrupting these processes); 2) polarize and weaken social cohesion; 3) cultivate a feeling of generalized suspicion, confusion, and disorientation; and 4) undermine trust in institutions, in democratic processes, in facts, and in knowledge.

Perhaps the greatest danger of disinformation understood in this strategic, and not opportunistic, sense resides in its capacity to hijack public conversation in democratic societies altogether (its dominant themes, narratives and frames) and turn agenda-setting, framing, priming, and narrative building into instruments of power. Under conditions of hybrid attack on the communication and sense-making infrastructures in a democratic society, factual, reality-grounded conversations become less practical and, worse, not even desirable. The path that has led to the current situation, where democratic, open societies seem under constant attacks that seek to disrupt their epistemic integrity, has a long and winding history, and dissecting it thoroughly is beyond the scope of the present analysis. Nevertheless, it is our understanding that a considerable part of the problem lies in the emergence of a new, largely ungoverned online information space, systemic risks to which remain poorly understood. This new, hyper-connected, technologized, and digitized realm has become the vulnerable strategic underbelly of modern democracies. These new information networks, which are the result of the interplay between mainstream media, social media, and, lately, AI and machine learning, have "created a tunnel to the center of our vulnerability, usable by any nation or collective of individuals at their discretion." While democratic societies are challenged by their adversaries in many fields, the fact remains that the most audacious, and most damaging, challenges are posed in these new the information and communication spaces. This is arguably the most spectacular geopolitical development of the post-Cold War period.

"Hybrid wars must be won long before they are waged"

Confusion between the two understandings of hybrid warfare described above represents a major source of vulnerability in terms of assessing the threat, in addition to planning and implementing adequate responses. One can think of the situation where a hostile state actor acts according to the tenets of the latter paradigm ("total political war" waged with non-military means, excluding or replacing kinetic action altogether), while the deployed threat response was conceived along the tenets of the former paradigm (hybrid warfare understood as actions preceding a traditional military invasion as such). In other words, the threat and the corresponding actions would target policy-making, public opinion formation, and sense-making processes, avoiding kinetic confrontations, while the threat perception and response would be traditional in nature (e.g., buying more weapons, increasing military build-ups, preparations for military mobilization, with some marginal attention paid to information warfare and disinformation operations understood as opportunistic and tactical in nature).

This hypothetical provides, albeit in simplified form, a more or less accurate approximation of the response of the democratic world to actions deployed by its current geopolitical competitors. Such intellectual myopia leaves targeted societies vulnerable to further and more effective attacks, while leaving room for complacency, and unwarranted definitions of "success" or "victory" (e.g., "see, we've been successful in deterring our enemy," "we have not been invaded after all," "we panicked over nothing," "the danger has been overblown," or "it's merely hysteria and war-mongering," among other hypothetical assertions). Such misplaced reactions are particularly risky, as they may indefinitely postpone the moment of realization, the wake-up call as to the magnitude of the threat, and of the systemic vulnerabilities exploited by hybrid warfare-as-warfare. Leaving aside all of the terminological hassle, the biggest misunderstanding, amplified and weaponized by disinformation in the first place, is entertaining the illusion that hybrid warfare is *less than warfare*.

Following the ideas put forward by Luke Coffey, if governance processes (meaning, by and large, policy-making, opinion formation, and sense-making in a democratic society) are the new battlefield, then responses must be adapted to this transformation. They should follow a "whole-of-society approach," but not at the expense of strategic, high-level and integrated government action. The response should consider the whole society inasmuch as hybrid warfare targets society as a whole. This does not preclude the design and preparation of military actions, or the creation of hierarchical or centralized structures and institutions within government for the execution of effective response. If hybrid warfare is not a lesser, "softer" type of warfare, displacement of government responsibility and empty calls for the involvement of "civil society" or "academia" may simply become part of the growing problem. Effective responses to hybrid warfare, seen and understood as no less than warfare, are not a simple matter of giving people more or "better" facts, literacy skills to navigate the turbulent information environment more safely, occasionally exposing a few bots and trolls, naming and shaming some dubious actors, flagging and down-ranking problematic online content, or assigning opaque credibility scores.

To be clear, such tactical initiatives are all very important, but a whole-of-society response to hybrid warfare as warfare remains a collective, strategic responsibility, requiring a whole-of-government, inter-institutional, trans-, and multi-disciplinary approach. This must involve government structures and institutions, law enforcement, mass media, the military, intelligence organizations, financial and business institutions, technology companies, academia, and the expert class writ large. This type of whole-of-government and whole-of-society approach, which must be implemented abiding to democratic principles, checks and balances, transparency, and the rule of law, has the potential to offer a systemic answer to the systemic problem of hybrid warfare. It places the focus on the quality of policy-making and sense-making processes, on the legitimacy (both in terms of inputs and outputs) of governing action, and on the underlying epistemic integrity of society. In simplest terms, good governance, and the perception of good governance, are the best resilience-building and resilience-enhancing measures. A well-governed society, which, *inter alia*, is able to maintain its epistemic integrity and the integrity of its information and communication space, is a resilient society.

This approach, we hope, appears pretty straightforward. However, we share the concern of Coffey, who warns that hybrid warfare can only be prevented, and not "won." Once the social, economic and political (i.e. both policy making and public opinion formation) conditions that allow for the deployment of hybrid actions are met–poor governance, poor input and output legitimacy, low trust, enhanced cognitive and emotional polarisation, a disregard for facts, and for the value and usefulness of facts-based discourse–it is probably too late to come up with adequate responses. In short, "hybrid wars must be won long before they are waged." As a result of mixing two paradigms to thinking about hybrid warfare and, in general, of misunderstanding the phenomenon as "less than warfare", the Western, democratic world gets more entangled every day in distracting and irrelevant policy disagreements (both at the individual country level and transnationally), gets stuck on the idea of "fixing the problem," and is left unable to formulate a vision adapted to new technological, social and geopolitical realities. It makes preparations for a war that, most likely, won't actually be waged in conventional form and has not been declared as such by its adversaries. At the same time, it dwells in systemic conceptual incoherence, misunderstands the nature of the threat, and does not adequately prepare itself and its citizens against a war, the hybrid war, that may be already underway.

About the Authors

Professor Alina Bârgăoanu is a Romanian communication scholar with a strong interest in digital transformation, strategic communication, fighting disinformation, and regulation of the digital eco-system. She is the Dean of the College of Communication and Public Relations, National University of Political Studies and Public Administration, Bucharest. She is currently a member of the advisory board of the European Digital Media Observatory and an affiliate member of the European Center of Excellence for Countering Hybrid Threats, Helsinki. In 2018, she served as a member of the High-Level Expert Group on Fake News and Online Disinformation at the European Commission.

Dr. Elena Negrea-Busuioc is an Associate Professor at the College of Communication and Public Relations, National University of Political Studies and Public Administration, Bucharest. She has been involved in several research projects on metaphors in communication, public opinion, populist communication, and hate speech in social media

The views expressed in these articles are those solely of the authors and do not reflect the policy or views of the Irregular Warfare Center, Department of Defense, or the U.S. Government.