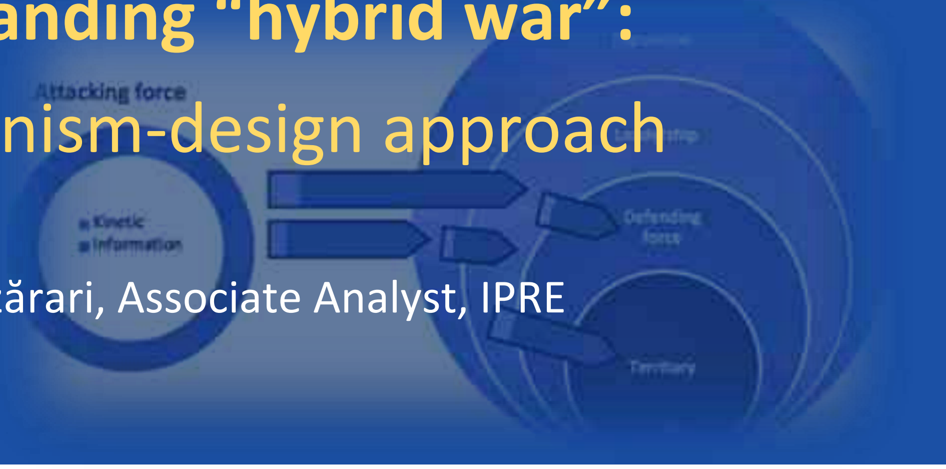
IPRE
Institutul pentru Politici
şi Reforme Europene
ipre.md

Deriving an Effective Early Warning Mechanism for Addressing Hybrid Threats

DEC 2020

Understanding “hybrid war”: A mechanism-design approach



POLICY PAPER

Dumitru Mînzărari, Associate Analyst, IPRE

Executive Summary

A hybrid aggression allows a foreign actor to technically become a domestic actor in the target state, avoiding detection and the costs imposed by international law for interstate aggression.

Building an early warning system for any type of threat requires a good understanding of that threat, which includes its signals, manifestations, means, targeted domains, and the impact it generates. To be able to do this we need to understand the hybrid war dynamics and mechanisms. This is the main focus of current analysis. It argues that the hybrid war targets specifically population (and political leadership), aiming to influence its perceptions (beliefs) and consequently its behavior.

Then, this influence is exploited to affect, influence or alter the political leadership, which consequently allows changing the internal and external policies of the target state. A hybrid aggression allows a foreign actor to technically become a domestic actor in the target state, avoiding detection and the costs imposed by international law for interstate aggression.

This aggression is done through the information operational domain of war and is facilitated by the lack of national borders in the information and communication spaces, which today is truly global. Building on this new understanding of hybrid war – as a logical foundation – we can then identify the logical bottlenecks and vulnerabilities of the hybrid type of interstate aggression.

This policy paper was published within the project “Deriving an Effective Early Warning Mechanism for Addressing the Hybrid Threats”, supported by the Dutch Embassy Office in the Republic of Moldova. The views expressed in this policy brief are the ones of the author only.

1. Where have we failed? The rationale for the new approach

The 2014 Russian aggression against Ukraine, with its annexation of Crimea and a proxy war in Donbas, has triggered a large debate on whether this has changed the face of modern warfare. Loosely defined terms and heuristic constructs like "hybrid war" and "gray zone" emerged to dominate the debate, which strived to understand and explain this Russian model of interstate aggression.

The notion of "hybrid war" is one the security policy analysts find to be the most elusive. Its definitions abound. Due to superficial understanding of the process behind the concept, and its excessive use, the "hybrid war" term risks to lose analytic value. A quick analysis will reveal that various countries and organizations attach different meaning to the concept. Some see it synonymous to cybersecurity, others – to foreign interference into electoral process, a third group prefer to equal it to disinformation and propaganda, while another group – with Russia's use of unmarked armed troops ("green men") in Crimea. These ad-hoc and non-systemic conceptualizations are determined by these actors' individual threat perceptions. However, in military parlance, these efforts respond to the means, rather than the ends of "hybrid war". As a recent study on this topic has challenged the existing orthodoxies – in line with this analysis - "Russia sees hybrid war as a type of conflict, rather than the means of waging it.[1]

The described misconception predictably generates a major policy challenge. How can we effectively address the security risks brought by the "hybrid war", if we are not clear about the mechanism behind that conflict technology[2]? The conceptual cacophony described above has dangerous policy effects. For instance, European Union, institutionally, prefers to talk about "hybrid threats" and descriptively focusses on the means of "hybrid war". Thus, it invests efforts and resources in responding to various actions, rather than focusing and addressing the goals of the aggressor waging the "hybrid war". This error is likely due to the Western culture of understanding interstate conflict through a mirror-imaging framework – viewing international competition through the binary logic of war and peace[3] and considering the competitors share that view.

As a first step, therefore, it is necessary to understand the ends of the opponents. Only thereafter we are able to assess the actions and try to elicit the significance and effect of its means. This difference is critical. If we focus on one specific (interstate) aggression action, we may fail to identify the attack materialized through a different set of actions. Or, we may

[1] M. Clark, *Russian Hybrid Warfare*, Washington D.C.: Institute for the Study of War, September 2020.

[2] I am going to use further in the text the term conflict technology or technology of aggression, to mean a "causal mechanism" of conflict process, drawing similarity from the economic concept of "technology of production". Coined by J. Hirshleifer in "The Microtechnology of Conflict", *Journal of Conflict Resolution*, Vol. 44, No.6, 2000, 773-792, a conflict technology takes the conflict efforts as inputs, uses a specific logical function to process these inputs, and based on them generates at the output a probability of victory or defeat. Therefore, the probability of victory/defeat depends not only on the quantity and quality of the input, but also on how these inputs are being employed (i.e. through a strategy or mechanism).

[3] C. Paul, "Confessions of a Hybrid Warfare Skeptic," *Small Wars Journal*, 3 March 2016.

fail to protect the correct targeted area. For instance, we may focus on addressing electoral interference during elections, while failing to address and undermine the opponent's more relevant influence operations preceding elections, which prepared that interference. Or, we might believe we need to address coronavirus-related disinformation, while missing that its main goal might be to cultivate citizens' distrust in authorities; or, for instance, to consolidate clusters of online audience for consequent influence operations. It is only by better understanding the main goals and then applying this knowledge to protect related targeted areas, that we can optimally address the effects of "hybrid war". It is only through that approach that we can make that conflict technology more costly, and thus less attractive to the aggressor.

The previously invoked effects are not just theoretical deductions. They are visibly emerging as ineffective policies. For instance, both NATO and EU assistance policy to Eastern Partnership countries is undermined by this approach. After asking Moldova to fill in a risk-assessment questionnaire, indicating its national "hybrid threats" related risks, the EU had consequently discarded the top concerns of Moldova. Instead, it elevated the concerns that are perceived important by EU states, such as cybersecurity. NATO took an identical approach, also focusing on cyber-defense assistance, predominantly. Cyber-attacks though, are in the context of hybrid war nothing more than supporting actions. They aim to either improve the knowledge about the targets of the attack[4], or soften and prepare the target for the forthcoming attack[5]. Moldova is under-developed from a cyber-management perspective and thus it has different counter-hybrid vulnerabilities and priorities.

Moldova is under-developed from a cyber-management perspective and thus it has different counter-hybrid vulnerabilities and priorities.

This analysis aims to present for scrutiny a conceptual framework that would improve our understanding of the interstate aggression model determined by "hybrid war" logic. To achieve this, it will compare and contrast the mechanisms of various war types, emphasizing the unique properties and qualities of the "hybrid" warfare. It will step back from the traditional (Western) focus on war, as a coercive policy and organized violence carried out by political units against each other.[6] Instead, it will propose to explore the broader idea of interstate aggression that aims to undermine or destroy a target country's sovereignty. In contrast to other types of war dynamics, it will introduce the idea that "hybrid war" is predominantly waged through the information operational domain and will explain the policy implications. Primarily, it will use the rationale of mechanism design. This means understanding the optimal rules that guide the process of various conflict technologies (including of the "hybrid war"), as well as the limitations imposed by various types of societies on these rules. It shall also account for the fact that an aggressor would like to optimize its behavior based on the two above-listed general conditions[7].

[4] For instance, the cyber-attacks against German Bundestag are likely to have been information collection efforts, to build behavioral profiles of German politicians and public functionaries, for their further targeting through the informational domain.

[5] Learning how to acquire control over electric grids, etc., would fall under this category; collapsing the electric grid or other services that endangers the livelihood of population allows to increase its insecurity, and thus susceptibility to attacks via information operational domain.

[6] H. Bull, *The Anarchical Society*, New York, Columbia University Press, 1977.

[7] For a more detailed (non-technical) explanation, see the intro chapter of T. Borgers, *An Introduction to the Theory of Mechanism Design*, (Oxford: Oxford University Press, 2015).

Building on the logic of these concepts, the analysis will break down the "hybrid war" problem into the following logical threads: 1) how the conflict technology widely-referred to as "hybrid war" operates; 2) whether it carries meaningful policy-relevant differences from other technologies of conflict (such as conventional or proxy wars), and 3) whether these differences require a distinct policy response.

2. Assessing the evidence of "hybrid war"

When analyzing Russia's invasion of Crimea, the most attention is drawn to the highly visible movement of armed troops in unmarked uniforms. Less attention was paid to the reason why these military groups faced little to no armed resistance. Failing to account for this key factor would lead to a faulty analysis. We will be missing an essential element of the hybrid war mechanism – the role of the population.

The population has become the most formidable obstacle against foreign military invasions – it is impossible to coerce it into compliance unless one is ISIS,[8] and it is not feasible to persuade it unless the local armed resistance is weak. The latest military operations, including those in Afghanistan and Iraq, suggested that destroying the opponent's organized military resistance, in the era of nationalism and even partially operating international law, is unlikely to achieve one's strategic objectives. In building the logic behind its version of "hybrid war" Russia's military planners explored the experience of the US and its allies in these two conflicts, along with its own lessons from Afghanistan and, more recently, Chechnya. Because of their costs, wars in the modern world are not even formally declared any longer,[9] making Grotius' definition of war (a legal condition between juridical equals) obsolete. Empirical observations suggest that classical infringements against another country's sovereignty, such as military territorial conquests, have become less frequent since 1945,[10] partially due to the costs imposed by the body of international norms regulating interstate warfare, such as the UN Charter.

That is, conventional wars are becoming increasingly costly, for many reasons – the domestic audience costs as well as the international pressure in economic and political terms, being the most obvious. Another important reason for this cost is the prohibiting penalty demanded by the goal of effective control over the sovereignty of the target country. Departing from this idea, the ability to either control the population of the target country or discourage it from violently opposing the aggressor has become a key element of "hybrid war". Population thus emerges as the center of gravity of this type of interstate aggression.

Russia's operation in Crimea was successful specifically because the population did not mount armed resistance. To the contrary, some groups assisted the Russian special forces

[8] Russia has displaced and coerced populations that resisted its policies in Chechnya, South Ossetia, Crimea and in Ukraine's eastern regions of Donetsk and Luhansk.

[9] T. Fazal, "Why States no Longer Declare War", *Security Studies*, Vol.21, No.4, 2012, 557-593.

[10] B.A. Lacina *et.al.*, "The Declining Risk of Death in Battle", *International Studies Quarterly*, Vol.50, No.3, 2006, 673-680.

that were publicly presented as local militia, to discourage Ukrainian military from fighting against the invasion. It did so by being organized to surround and isolate Ukrainian military bases, blocking access roads and areas, serving as human shields for Russian soldiers, and creating the image of popular support for the fake anti-Kyiv uprising that served as the smokescreen and cover for the Russian military invasion.

Crimea is difficult to interpret this way, if one does not know what to look for – due to misunderstanding the aggression mechanism. In the Crimean case, the Russian military did not have to prepare its ability to influence and exploit population groups in the target territory, like it needed to do in Donbas, Odessa or Kharkiv. It is important to understand that depending on the operational objectives, an aggressor may only need the support of a small but very politically active group of the population. For instance, de facto in Crimea only some 30 percent of the population participated in the Russia-organized referendum, and reportedly only half of them voted as desired by Moscow.[11] However, because Russia controlled the terrain, and has replaced the local governance, it operated basically as a domestic political actor.

Therefore, the goal, and the first stage of a "hybrid war", is to use the population to question the legitimacy of the target state's government. This allows to camouflage an external aggression as a domestic rebellion. In Donbas, the support of the population for Russia's infiltrated armed groups[12] was smaller than in Crimea. This allowed for population groups loyal to Kyiv to mount counterdemonstrations and resistance. It bought time for the Ukrainian law enforcement to react and either organize armed response or quell the Russia's improvised rebellion, in particular in Kharkiv.[13] A second stage, and a direct consequence of staging "popular uprisings", was replacing the local administration with people dependent on or loyal to Russian forces. This explains the earlier claim that Russia could gradually operate as a local (Ukrainian) political actor through replacing local authorities. It consequently escalated, when confronted with Ukrainian armed response, through the creation of "peoples' republics". This is the next element of Russia's model of "hybrid war", applied usually in case of escalation. It allows to obscure Russian military presence by disguising the foreign aggression through the misapplication of self-determination principle of international law.

The critical role of population, as the critical target in the "hybrid war", has been recognized by both political and military actors in Russia. In a discussion with Jim Rutenberg, a New York Times political correspondent at that time, Dmitri Peskov, Putin's press secretary[14], provided a very vivid clarification. Due to its importance, it deserves to be presented in its extensive form:

> "The transformation and acceleration of information technology, Peskov said, had unmoored the global economy from real value. Perception alone could move markets or crash them. 'We've never seen bubbles like we've

[11] S. Pifer, "Crimea: Six Years after Illegal Annexation," The Brookings Institution, 17 March 2020.

[12] I. Zolotuhina, *Voyna s Pervyh Dney*, Kyiv: Folio, 2015, 70.

[13] BBC.com, "'HNR': Har'kovskaya Neudavshayasya Respublika," 8 April 2015.

[14] The New York Times, "RT, Sputnik, and Russia's New Theory of War," 13 September 2017.

> seen in the greatest economy in the world, the United States,' he said. The same free flow of information had produced 'a new clash of interests,' and so began 'an informational disaster — an informational war.'
>
> By way of example, he pointed to 'this girl, from show business, Kim Kardashian.' Kardashian is among the most popular people in all of social media, with 55 million Twitter followers, nearly 18 million more than President Trump. 'Let's imagine that one day she says, 'My supporters — do this',' Peskov said. 'This will be a signal that will be accepted by millions and millions of people. And she's got no intelligence, no interior ministry, no defense ministry, no K.G.B.' This, he said, was the new reality: the global proliferation of the kinds of reach and influence that were once reserved for the great powers and, more recently, great media conglomerates.
>
> Even Peskov sounded slightly amazed considering the possibilities. '*The new reality creates a perfect opportunity for mass disturbances*,' he said, '*or for initiating mass support or mass disapproval*'".

Obviously, Peskov only reflected what Russia's political and military experts briefed to Kremlin. An often misinterpreted and incompletely understood reference is the so-called Gerasimov doctrine, named by Russia's Chief of the General Staff, General Valery Gerasimov[15]. I argue that the critical idea of the Russia's chief of defense is the following one:

> "The focus of employed conflict methods is shifting towards a wider application of political, economic, informational, humanitarian and other non-military measures, which are *implemented through the triggering of the population's conflict potential*".

In fact, one could argue that a more accurate description of what is referred as "hybrid war" after 2014 Russia's invasion of Ukraine, would be population-domain or human-domain war.[16] U.S. military explored the concept at the tactical-operational level in Afghanistan, under the conceptual label of "human terrain" and its "hearts and minds" approach. There is little doubt that the Russians considered the American experience and developed the concept for strategic-political level. They also considered the rich Soviet experience of inciting and supporting armed rebellions. But make no mistake – the current approach differs in a very important way.

If in the past foreign aggressors would drop leaflets, infiltrate spies and use *agents provocateurs* to try and influence limited segments of elites or groups of population in the target state, modern technology gives a foreign actor unimpeded access to the whole population, which never in history was ever possible. The globalization of mass media and communication operates as an enabler by creating a borderless informational domain; it

[15] Valery Gerasimov, "Tsennost' Nauki v Predvidenii", *Voyenno-Promyshlennyi Kuryer*, 8 (476), 27 February 2013.

[16] C. D. Wood, "The Human Domain and the Future of Army Warfare: Present as Prelude to 2050," *Small Wars Journal*, 8 February 2016.

has made it technologically possible to target foreign populations at a previously unimaginable scale.[17] This is a factor that makes the "hybrid war" technology of aggression distinct from the past uses of disinformation and propaganda. As an example, Russian military strategists point out that "no goal will be achieved in future wars unless one belligerent gains information superiority over the other", and that "armed struggle has expanded from the ground, sea, and aerospace into an entirely new environment – information".[18]

The revolution in social sciences made possible by the availability of Big Data[19] is another effective enabler for this conflict technology, as the Cambridge Analytica – Facebook scandal has revealed.[20] There are no national borders in the communication and information spaces, which transforms the information space in a separate operational domain of warfare. And because of this, understanding war in information-operational domain requires a different conceptual framework, a different operationalization, different forces and capabilities, as well as a different set of skills. It would be hardly possible for Russia's opponents to be able to fully understand its "hybrid war" model and effectively respond to it, unless they designate informational space as another synthetic operational domain of war, in addition to the existing cyber, and the physical operational domains such as land, air, naval and space.[21]

This view on interstate war is rather new to Western policymakers and experts. Only more recently some rare voices emerged to defy the existing conventional wisdom, calling for reconceptualization of modern interstate conflict generally and Russia's model of "hybrid war" in particular. For instance, Stanford's Amy Zegart forcefully argues that U.S. is trying to understand modern conflicts by applying "outmoded theories from a bygone era".[22]

Given this, there is no wonder that existing policy and academic literature continues to severely misinterpret some of the existing conflicts in post-Soviet area as "ethnic", when in fact strongly resemble the Russian aggression against Ukraine. To a large extent this was due to their time overlap with the conflict in former Yugoslavia, as well as the Soviet and consequently Russia's efforts to present them as identical to the Balkans inter-ethnic conflicts. It was a convenient cover-up for justifying Russian military involvement. Therefore, there was much less Western scrutiny of Russia's actions in post-Soviet space in the early 1990s, and Moscow skillfully used its influence in international organizations to push for its interpretation of the conflicts. For instance, the OSCE predecessor organization –

[17] D. Minzarari, "Coronavirus Pandemic Impact on Modern Conflict and Future Warfare," in T. Tardy (ed.) *COVID-19: NATO in the Age of Pandemics*, NATO Defense College Research Paper, No.9, May 2020, 41-49.

[18] S. G. Chekinov and S. A. Bogdanov, "On the Nature and Content of the New-Generation War", *Military Thought*, No.10, 2013, 13-24.

[19] "The Age of Big Data," *The New York Times*, 11 February 2012.

[20] "The Cambridge Analytica Scandal Changed the World – but It Didn't Change Facebook," *The Guardian*, 18 March 2019.

[21] D. Minzarari, "The Interstate Conflict Potential of the Information Domain," *Policy Brief* (forthcoming October 2020), NATO Defense College.

[22] Amy Zegart. "The Race for Big Ideas is On," *The Atlantic*, 13 January 2020. See also P. Roberts, "Designing Conceptual Failure in Warfare," *The RUSI Journal*, Vol. 162, No. 1, 2017, 14-23; T. Wesley, "Multi-Domain Operations and Lessons from NSC 68 in the Competitive Space," *The RUSI Journal*, 5 October 2020. Other contributions to the emerging debates include Clark (2020), Minzarari (May 2020; October 2020).

Conference on Security and Cooperation in Europe – legitimized the Russian's interpretation in its notorious "Report 13". Among other erroneous claims it stated that:

> "The breaking up of the Soviet Union and its replacement by Russia, eleven successor states (one of them Moldova), and the Baltic countries, was followed by a revival of ethnic and other antagonisms which political wisdom has not always succeeded in dissipating. As a result, some areas, among them Transdniestria, have thought it fit to attempt secession from their post-Soviet state and the establishment of mini-'states' of their own."[23]

A more thorough assessment of the Soviet media in 1989-1991 would uncover a picture, revealing that Transnistrian conflict has lots of similarities to the 2014 Russia's political manufacturing of armed rebellions in Donbas. What was somewhat different was the fact that Moldova's Transnistrian region at that time resembled Crimea in terms of the numbers of population loyal or controlled by Moscow. For instance, on 16 August 1989, the directors of several major factories in Transnistria, including "Elektrofarfor", "Elektroapparatura", and the machine-building plant, called the workers councils to strikes. They were encouraged to do this and supported by the Russian-speaking communist party officials in Bender and Tiraspol, who opposed the Romanian speaking authorities in Chisinau.[24]

The strikes against central authorities in Chisinau were coordinated and guided by the Interfront movement, which according to KGB head Vadim Bakatin were conceived by his organization to create tensions in the Soviet republics and put pressure on the leaderships that wanted to leave the USSR.[25] The USSR leadership had good control over the industrial complex in Transnistria – and its numerous workers collectives – and therefore it could effectively engage the factory directors. In fact, the first Moldova's president, Mircea Snegur, recalled in his memoirs that he received threats during his meeting with Mihail Gorbachev and Anatoliy Lukyanov[26] in 1990. Gorbachev confronted him with an ultimatum, saying that if Snegur was not going to sign the new Union Treaty, he would have to deal with separatist entities in Transnistrian and Gagauzian regions of Moldova.[27]

Consecutively, Moscow ordered its military units in Transnistria to give armament to the „opolchenie" groups, the "Republican Guard" it created, as well as the Cossack units that it deployed to Moldova, for protecting the separatist Transnistrian administration. During the short violent conflict in Transnistria, the Moscow-controlled military units directly fought the Moldovan forces, forcing Snegur to capitulate and sign with Russia's President Boris Yeltsin the 1992 cease-fire agreement.

This is why it is useful – when analyzing various conflicts in post-Soviet area – to examine the conflict mechanisms through adopting an abstract approach. The tools used in

[23] CSCE Mission to the Republic of Moldova, "Report No. 13," 13 November 1993, p.2.

[24] D. Minzarari et al, "Rol' Rossiyskoy Federatzii v Razreshenii Pridnestrovskogo Konflikta: Chast' Pervaya – Upadok SSSR i Zagovor Tzentra," *Azi.md*, 26 March 2007.

[25] V. Bakatin, *Izbavlenie ot KGB*, Moscow: Novosti, 1992.

[26] The Chairman of the Supreme Soviet of the USSR. Lukyanov is believed to have been a leading force behind the 1991 coup against Gorbachev.

[27] M. Snegur, *Labirintul Destinului*, Draghistea, 2007.

Transnistrian conflict might seem different from those in Ukraine's Donbas, due to seemingly different conditions. However, they aimed to implement a conflict mechanism of significant similarity. In Ukraine's Crimea and Donbas, we witnessed a segment of the population being loyal to Russia, along with some local elites. Russian military planners only had to explore that population's segment to create the appearance of a rebellion and contest the legitimacy of central Kyiv authorities. Then, they replaced the local administration in the regions targeted for physical control. In the Transnistrian region of Moldova, Russian planners controlled most of the local party elites and factory directors. Moscow used that control to organize the region's numerous workers for strikes and protests against Moldova's central authorities. It aimed to achieve an identical goal – to delegitimize central authorities and create armed groups for establishing administrative control over the secessionist territories. In both cases, it aimed to show that driving force behind the secessionist movement was the inter-ethnic tension and resulting insecurities, rather than Russia's security services and the military.

3. Deriving the conflict mechanism

War is generally defined as a coercive policy tool that forces the opponent to give up the contested good, which may be territory and control over resources, or a policy stance. If diplomacy could be compared to a process where we negotiate to buy or barter a desired good from another country, war would be similar to a robbery. War involves either the use of force or the threat to use force and is understood to basically operate as a process of mutual attrition[28] of war-related resources, such as military troops, hardware, and supporting materials. The underlying mechanism of the classical war technology is to overcome the resistance of the opponent's armed force. The latter serves as a physical obstacle between the aggressor and the goal – control over territory, which consequently allows to exert control over resources or political leadership. The proxy war is driven by a similar logic of mutual attrition of resources. The difference is in the reduced political exposure of the aggressor, who is still operating by supporting an existing armed opposition against the target government. The core operation domain is usually land, though other physical domains, such as air, naval, and space may be used in conventional war. Cyber and information operations will come solely as efforts supporting the main kinetic endeavor.

The "hybrid war" conflict technology explores though a different underlying logic. Its main aim is to influence the behavior of the target government (in favor of Russia's strategic aims), not through direct kinetic actions, but by creating political pressures and costs and using domestic actors and tools. The conventional war aims to take control over the territory, so that it can acquire as a result control over population and political leadership. The "hybrid war" directly targets the other two elements of state sovereignty – population in particular and the government. The aim though is exactly the same – to undermine the sovereignty of the target state, in particular aiming to influence policies. Importantly though, hybrid warfare is able to deliver control of the target state's territory, which only conventional territorial conquest can offer. That is, hybrid warfare can be a full-fledged alternative to conventional

[28] J. Hirshleifer, "The Macrotechnology of Conflict," *Journal of Conflict Resolution*, Vol.44, No.6, 2000, 773-792.

war. Hybrid warfare preponderantly weaponizes information, in its direct targeting of population, leadership, or both (fig.1). The military tool and kinetic actions are used only in support of the major effort of information operations. It is the other way around in conventional and proxy war cases.

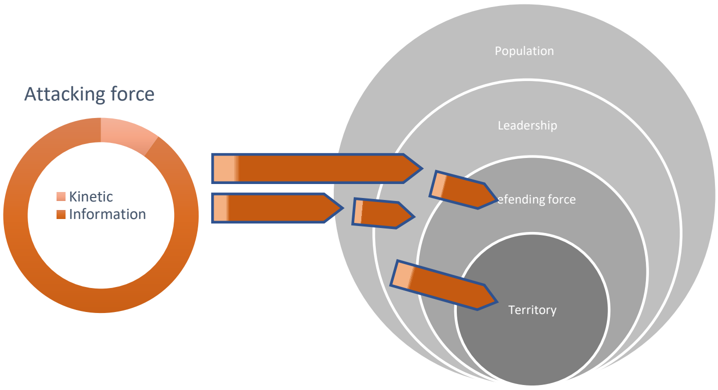


Fig.1: The mechanism of hybrid war as a policy tool[29]

By acquiring control over or the ability to direct the population of the target state, or its leadership, the attacker can advance its objectives. These could include reducing funding for the target country's military, pushing into leadership positions in the military and intelligence agencies incompetent people, or making the target state withdraw from military and political alliances, or join their previous competitor.

To understand hybrid warfare better, we should also look at its microdynamics. A common error is to believe that it can only be applied to countries that have a national minority of the same nationality as the attacker's main population. The Russian annexation of Crimea comes to mind as the classical modern example. However, the objective in hybrid war is not necessarily to make the population of the target country become loyal to the attacker. The most frequent approach would be to antagonize the population against an outcome that the attacker would like to avoid. For instance, Russia is investing significant resources to influence beliefs, perceptions and – consequently – actions against NATO and EU, including among the members states of these organizations. Or, it works to create chaos, turmoil or economic hardship in the target country, so that it is easier to bring into power a new political leadership that is more likely to advance the attacker's favorite goals.

Western military and security planners do not seem to understand the mechanics of these actions, their potential effects, and thus consider them outside of the war context. They tend to view the "hybrid war" actions as being in the low-intensity, pre-war part of the conflict escalation specter. As some analysts suggest, this view is ignoring the fact that Russian military thinking has a holistic view towards warfare. According to Adamsky, this paradigm does not aim at "the annihilation of the enemy system by methodical destruction of its forces, but seeks its dismantlement and disintegration through fragmentation, paralysis and

[29] Part of the research, aiming to understand the dynamics of "hybrid war" was conducted in the framework of author's research fellowship at the NATO Defense College in Rome, from March to August 2020.

neutralization.[30] He insightfully emphasizes (using the Syrian case) that Russia does not prefer to engage into a large-scale operation, but a comprehensive and holistic one, which mixes kinetic and non-kinetic tools, hard and soft means of power, aiming to reverse strategic trends, fragment and neutralize opposition, and facilitate conditions for a favorable political process. However, kinetic element is fully subordinated to the information operational domain effort, which represent the core effort of the "hybrid" conflict technology.

Using the logical framework of contest success functions and mechanism design, we could suggest that the key war effort in "hybrid" contest is represented by influence operations that focusses on creating tensions, disagreement, and conflict between the population and the authorities of the target country. Disinformation, cyber-attacks, economic sanctions or even the instigation of armed rebellions are targeted towards creating this tension, decoupling the population from the government. It is therefore an accurate metaphor to call "hybrid wars" as "population-domain wars".

4. Impact on policy-making

What is the pressure of this technology of interstate aggression on national security and defense policies? It requires a total and fundamental review of the logic of interstate conflict. What Western military and security thinking on war views today as conflict in the "gray zone" – below the threshold of war, is actually viewed by Russia as war. Because Russian military has a holistic view on interstate conflict, it mixes effectively both kinetic and non-kinetic tools, being able to move from one end of the conflict specter to another, depending on operational needs and strategic objective.

It does not send armed divisions across the border to topple and replace an unfriendly government with a more suitable one or loyal. It will instead design and implement influence operations targeting critical segments of the population to influence and even participate in the target country's political process. As Gerasimov and other Russian military professionals and thinkers suggested, the outcome may be identical to that of an armed aggression, but at significantly lower costs. Soviet Union invaded Hungary and later Czechoslovakia to maintain them in its sphere of influence. Russia invaded Georgia, though failed to achieve this.

It has high hopes to be able to block Moldova's further gravitation towards European Union and instead bring it into Russia-led regional structures, using a mix of implied military threats and influence operations. Moldova's President Igor Dodon videoconference with Vladimir Putin and the consequent rollback of Tiraspol's decision to block the participation of Transnistrian inhabitants in presidential elections in Chisinau is a strong signal in this regard. If there were any doubts, the recent Lavrov's interview is very telling. He accused the United States of "attempting to create 'an abscess' in Moldova by pushing for a total victory of pro-Western political forces".[31] These actions, which are costly signals in foreign policy, are indicating the very significant Russian involvement in ongoing electoral process. This involvement is a replacement of an invasion similar to those in Hungary, Czechoslovakia or

[30] Quoted in D. Adamsky, "Russian Campaign in Syria – Change and Continuity in Strategic Culture," *Journal of Strategic Studies*, Vol 43, No.1, p. 108.
[31] "Bol'shoe Interv'ju Sergeya Lavrova Trem Radiostantziam: Polnaya Stenogramma," KP.ru, 14 October 2020.

Georgia. In case of failure, it is likely to employ a strategy similar to Crimea, instigating and supporting radical and violent opposition to a government it considers unfriendly.

This demands a review of national defense and security policies. It requires their reconceptualization, and the design of more suitable paradigms, tools and actions to effectively respond to the described "hybrid" conflict technologies. If Moldova can lose its sovereignty as a result of foreign influence operations, conducted as part of a "hybrid war", it makes sense to prepare to understand, anticipate and effectively undermine them.

This analysis argues that an aggressive country can achieve the level of control over a target country through "hybrid war" means that is identical to that allowed by a conventional war. It describes he mechanism, tools and effects of the "hybrid" conflict technology and provides examples. It reinterprets actions like electoral interference, disinformation and propaganda to be just separate elements of "hybrid war" that can't be countered outside of a holistic approach. And, it provides the conceptual framework to consider developing countermeasures, starting with a system of early warning measures.

An effective response to "hybrid war" conflict technology cannot exist without early warning. "Hybrid" aggression is difficult to detect, given its use of domestic processes and the ability of aggressor to infiltrate the domestic political process of the target state. If a response is to achieve success it must, necessarily, involve an early warning mechanism, which would identify the elements and stages of the "hybrid" aggression. This analysis represents the logical foundation for deriving such an early warning mechanism.

5. Conclusions: Preparatory steps for EW

Building an early warning (EW) system for any type of threat requires a good understanding of that threat: its signals, manifestations, means, targeted domains, and the impact it generates. Based on this understanding experts design various threat assessments, which allow producing indicators to be monitored, assessed and analyzed. Depending on the scope of the EW mechanism and the available resources, the indicators' structure can be fine- or coarse-grained.

A major challenge though, as recognized by experts[32], is that we fail to well understand the hybrid conflict technology – or how the aggressor's efforts and resources, invested into waging a hybrid war, transform into the probability of its victory or defeat. To be able to do this we need to understand its dynamics and mechanisms. This is exactly what the current analysis has focused on. It argues that hybrid war targets specifically population, aiming to influence its perceptions (beliefs) and consequently its behavior. Then, this influence is exploited to affect, influence or alter the political leadership, which consequently allows changing the internal and external policies of the target state. This aggression is done through the information operational domain of war, and is facilitated by the lack of national borders in the information and communication spaces, which today is truly global.

[32] Rietjens, Sebastiaan, "A Warning System for Hybrid Threats – is it Possible?" Hybrid Center of Excellence Strategic Analysis 22, June 2020.

Equipped with this understanding we are able to conduct a more accurate and effective threat assessment, to understand the means, the ways, and the ends of the hybrid war. Building on this foundation, we can then identify the logical bottlenecks and vulnerabilities of a hybrid type of interstate aggression. Moreover, assessing the underlying condition of the potential target country, we are able to further increase the accuracy of this assessment. All of these steps and new knowledge allow us to address the challenges that experts identified to be preventing effective EW systems against hybrid wars. The next stage of the project will do exactly this – will build upon the identified hybrid war mechanism to create the framework of a hybrid war EW system, adjusting it to the specific conditions of the Republic of Moldova.

About the author

Dumitru Mînzărari, Ph.D., is an Associate Political Analyst at the Institute for European Policies and Reforms (IPRE, Chișinău) and Research Associate, German Institute for International and Security Affairs (SWP, Berlin). He received his PhD in Political Science from the University of Michigan-Ann Arbor, and his MA in International Affairs from Columbia University in New York. Dr. Mînzărari is a former military officer who served as state secretary for defense policy and international cooperation with the Moldovan Ministry of Defense, worked for the Organization for Security and Cooperation in Europe field missions in Georgia, Ukraine and Kyrgyzstan, and with several think tanks in Eastern Europe.

5 ani
Din 2015
IPRE
Institutul pentru Politici
și Reforme Europene
ipre.md

The Institute for European Policies and Reforms (IPRE) was established in March 2015 as an independent, non-profit and non-partisan think-tank. IPRE's Mission is to accelerate the European integration of the Republic of Moldova by promoting systemic reforms, enhancing participatory democracy and strengthening the role of citizens in national and local decision-making processes.

IPRE is a member of the National Platform of the Civil Society Forum of the Eastern Partnership (www.eap-csf.eu), co-initiator of the Eastern Partnership Think-Tank Forum launched in 2017 in Chisinau.

Address: București 90 street, of. 20
Chișinău, MD-2001, Republic of Moldova
Tel.: + 373 22 788 989
E-mail: info@ipre.md
Web: www.ipre.md