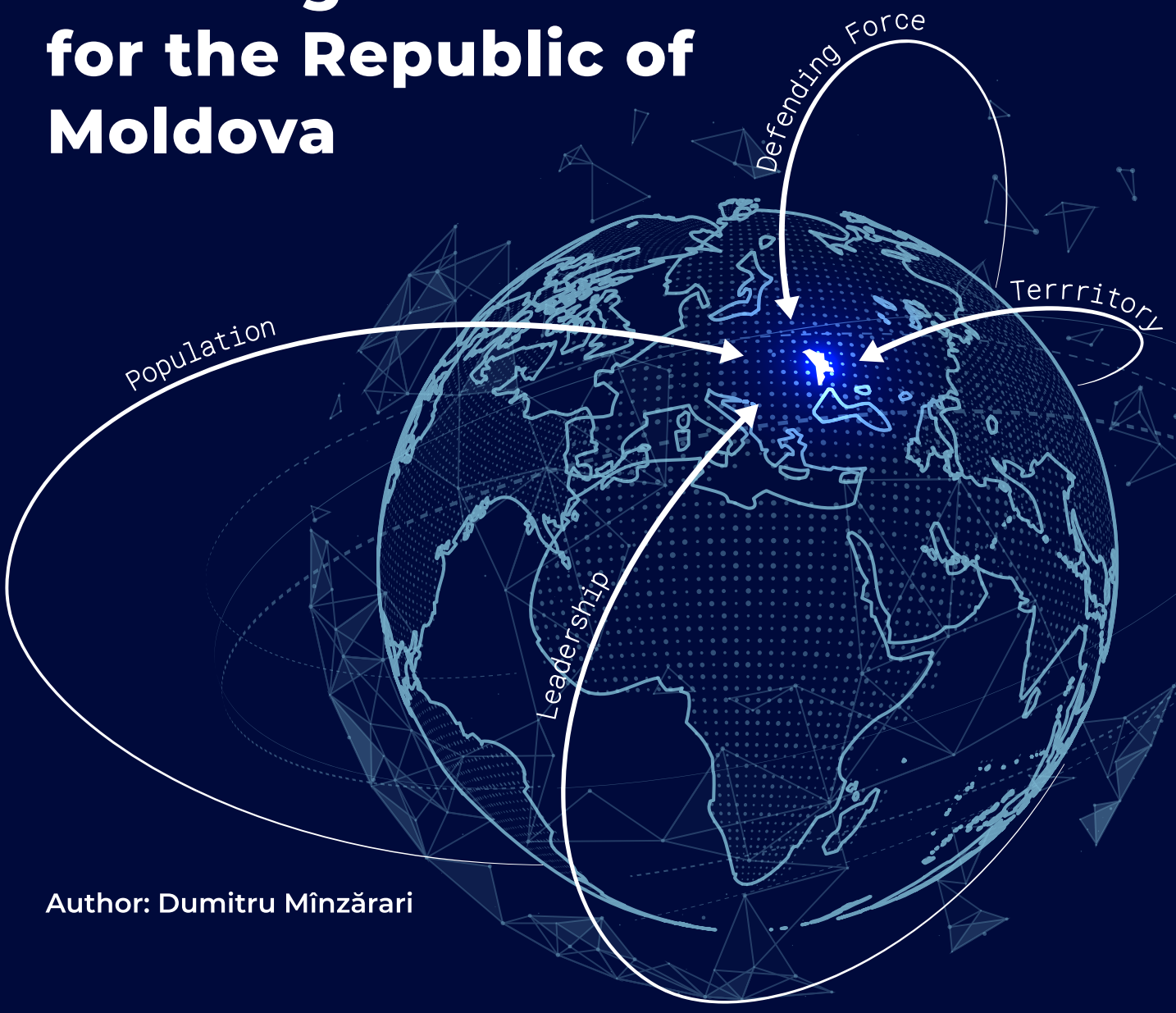
IPRE
Institute for European Policies and Reforms
ipre.md

Kingdom of the Netherlands

# A Hybrid War Early Warning Model:

## Towards an Early Warning Mechanism for the Republic of Moldova




Author: Dumitru Mînzărari

March 2021

**Acknowledgements:**

*This Study is published within the project "Deriving an Effective Early Warning Mechanism for Addressing the Hybrid Threats", implemented by the Institute for European Policies and Reforms (IPRE) in partnership with Dr. Dumitru Mînzărari, Associate Political Analyst at IPRE (author) and Dr. Arlinda Rrustemi, Strategic Analyst at the Hague Centre for Strategic Studies (HCSS) (peer-review expert). IPRE is grateful for their contributions, as well of the other experts that provided their views and inputs at the workshops and other online events organized during the preparation, validation and presentation of the study. We are in particular thankful to Bas Rietjens, Professor of Intelligence & Security at the Netherlands Defence Academy, Vilmos HAMIKUS, Head of Hybrid Threats at the Service at the European External Action Service (EEAS) and Andras RACZ, Senior Fellow, Robert Bosch Centre for Central and Eastern Europe (DGAP). We would like also to thank the Embassy Office of the Netherlands in the Republic of Moldova, the Embassy of the Netherlands in Romania and the Government of the Kingdom of the Netherlands for the supporting this action.*

**Disclaimer:**

Kingdom of the Netherlands

*This Study is published within the IPRE project "Deriving an Effective Early Warning Mechanism for Addressing the Hybrid Threats", funded by the Embassy Office of The Netherlands in the Republic of Moldova. The views expressed in this Study are the ones of the author only.*

**Published by:**

**Institute for European Policies and Reforms (IPRE)**
Address: Str. București 90, of. 20, Chișinău
MD-2001, Republic of Moldova
T: + 373.22.788 989, E: info@ipre.md W: www.ipre.md

# TABLE OF CONTENTS:

## EXECUTIVE SUMMARY

*Designing and implementing an Early Warning Mechanism is charting new terrain for the Republic of Moldova. While separate and ad-hoc exercises are likely conducted at some governmental agencies, these are ineffective, unless they are conducted* ***systematically and consistently****. One of the largest values of this exercise is the* ***size and quality of the data****. Data is the asset that allows for effective decision making, which is even more critical to countries with scarce resources, like Moldova. To initiate an effective data collection and aggregation exercise, which would capture information useful to assess and analyze hybrid-war-related indicators, one would* ***require*** ***investments into resources, logistical and technical support, training, as well as a proper legal framework****.*

*A proper way to do this is to establish a designated early warning cell, as part of a* ***governmental institution that leads the national effort*** *to counter hybrid threats and activities. Having such a unit allows* ***to effectively deal*** *with the very challenging technical task of hybrid war early warning. First of all, this requires dedicated and trained personnel to conduct continuous* ***event and incident monitoring****, for data collection and aggregation. It also requires* ***trained personnel to conduct analysis*** *and interpretation of the hybrid war indicators****, to provide effective and timely advice to policymakers****. As more data will be collected and institutional knowledge about hybrid war mechanism and* ***indicators*** *will be consolidated,* ***parts of the process could be automatized****. Until then, the early warning exercise will depend upon and rely on* ***highly skilled subject area analysts with strong contextual knowledge****.*

*The early warning effort at the national level requires* ***coordination in terms of information requirements****, the* ***distribution of tasks across agencies*** *and the* ***consequent aggregation of their outputs****. This can be streamlined by generating* ***in-house information collection and collation capabilities for the governmental agencies with interest*** *and* ***capabilities against hybrid war threats****. It also requires, beside establishing the proper* ***legal framework****, addressing* ***the data protection****, as well as the* ***information and communication security challenges****.*

## INTRODUCTION

Building an operational crisis early warning (EW) mechanism is an **extremely laborious process, requiring significant intellectual and material resources**, as well as the ability to sustain it. This is why not many countries or organizations are able to implement such an ambitious action.[1] Another challenge relates to the **existing models' accuracy,** which is frequently questioned. The truth is that a crisis early warning mechanism is not a crystal ball – at least, not yet. However, such practical **exercises can be useful for planning and response purposes**, in particular since the monitored and expected crises are **high-cost negative events, justifying the investments**.

The current analysis is proposing a model of a hybrid-war-early-warning mechanism, targeted at the **monitoring, analysis, and interpretation of a set of tailored crisis indicators**. **It aims to facilitate governmental early response against hybrid war-related risks, threats, and activities**. I use conceptually the term "hybrid war" instead of "hybrid threats" as it is more accurate analytically - threat is a potential cause of harm, while there is evidence that the respective harm is already being done. **The mechanism is built on a general model of hybrid war**, **prepared based on the evaluation of Russia's hybrid activities in both developed and developing countries, including Ukraine and Moldova**.[2] Given the need for a **greater understanding and preparation of the Moldovan authorities against hybrid war**, employing such a mechanism would offer a set of benefits: **the anticipation of resources, training, and actions required to improve an effective response**; **the creation of response algorithms** allowing to reduce the time gap between observing the crisis event and responding to it; the **decrease in inflicted costs** that a crisis event is likely to generate; and the **increased chance to prevent an escalation to a more violent conflict**, given a properly designed early response.

The existing early warning and forecasting approaches are varied, **depending on their geographic scope, thematic scope, or methodological framework**. In general terms, an early warning mechanism consist of i**) data inputs, collected over a specific timeframe; ii) data classification by crisis indicators; iii) data analysis; and iv) data interpretation in terms of intensity of risk.** Most modern and sophisticated early warning models conduct all these steps **automatically**. Some analyze and interpret the data based on **tailored crisis models and matrices**[3], while others do it based on

[1] F. Barton et al., "Early Warning? A Review of Conflict Prediction Models and Systems," Center for Strategic and International Studies, February 2008, p.14-16.
[2] D. Minzarari, "Understanding 'Hybrid War': A Mechanism-Design Approach," IPRE Policy Paper, December 2020, http://ipre.md/wp-content/uploads/2020/12/Policy-Paper_Understanding-hybrid-war_Dumitru-Minzarari.pdf.
[3] M. Raith, "Addressing the Conflict Cycle – The OSCE's Evolving Toolbox," OSCE Insights nr.3, 2020.

**artificial intelligence tools**[4], which are preliminarily trained on **issue** or **area-specific large data sets**.

The current approach will use **a model-based early warning mechanism**. There are several solid considerations for favoring this choice. First of all, **building an automatic Artificial intelligence (AI) model was beyond the scope of the project**. Secondly, such an effort would require **ample data to train the AI model – the more data, the more accurate is the model likely to be**. A major challenge in conflict analysis is that we **do not have sufficient and accurate – or representative – data**. In fact, academic research increasingly suggests that **lack of sufficient and proper data needs to be mitigated with the use of models and solid theories**.[5] This is encouraged by observations that there are visible changes in the modern conflict dynamics, comparing to types of security challenges we observed in the past, and **it would be erroneous to use old approaches to address emerging challenges**.[6] Finally, the hybrid war, as an **emerging conflict technology**[7], has been **poorly studied and there is limited related data available**. This makes a theory-free approach to designing a hybrid war early warning mechanism being methodologically improper.

## 1. CRISIS MECHANISM

Before explaining the crisis mechanism, related to the hybrid war, it is necessary to offer some terminology clarifications. The European Union preferred terminology is "hybrid threats", which is a diplomatic term rather than a technical and analytic one.

The **diplomatic culture of EU cannot accept official use of "hybrid war"**, since this is perceived as accepting that th**e EU may be at war with Russia or other states that are using technologies of hybrid aggression** against the EU. However, the term "threat" is incorrect analytically. A threat is a potential cause of harm initiated by deliberate or accidental actions.[8] A threat is related to actions that have not yet been initiated but are expected. We can talk about the threat of artillery strikes before they occur, but after the artillery attack started, we cannot talk about "threat" anymore. It's an attack. Because - based on the employed hybrid war model, its elements are already visible in Moldova, Ukraine and other countries – the attack has been initiated, we cannot talk any longer about threats, but instead have to deal with actions.

[4] "Dynamic Global Conflict Risk Index," EU JRC Technical Report, 2019, https://publications.jrc.ec.europa.eu/repository/bitstream/JRC118701/dynamic_gcri_technical_report_1.pdf.
[5] **L.-E. Cederman and N.B. Weidmann, "Predicting armed conflict: Time to adjust our expectations?" Science 355(6324), 2017, pp. 474–476. Or, T. Chadefaux, "Conflict Forecasting and its Limits," Data Science, Vol.1, no.1-2 2017, pp. 7-17.**
[6] A. Zegart, "The Race for Big Ideas is On", The Atlantic, 13 January 2020
[7] D. Minzarari, "The Interstate Conflict Potential of the Information Domain," NDC Policy Brief nr.19, November 2020.
[8] See, for instance, the UN Security Analysis Handbook, p.10.

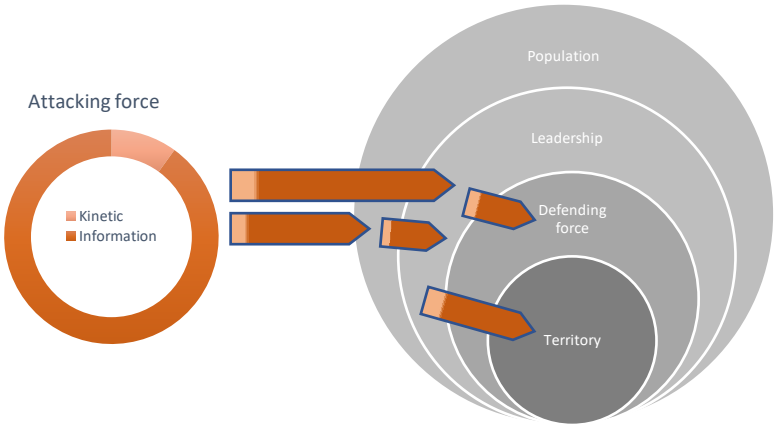



***Figure 1: The hybrid war mechanism[9]***

As an exception, it would be possible to talk about "hybrid threats" as separate incidents but not as a process. For instance, we may already be the target of the hybrid war but have not yet observed cyber-attacks. Then we can talk about the "hybrid threats" as possible incidents, in terms of cyber-attacks that are expected, but have not yet been noticed. In terms of the process, however, we will be in a state of hybrid war. In other words, we can talk about "hybrid threats" before the actions related to them are implemented, after which we should refer to the process as "hybrid war".

The proposed crisis mechanism for hybrid war is related to the observed transition of interstate aggression from the territorial invasion historical approach – as primary entry point into war – towards acquiring instead control over population and political elites (fig. 1). This has been found to be dominant interstate aggression models in Ukraine in 2014, and in the Republic of Moldova in 1992. It also reflects well the Russian hybrid aggression towards a number of developed countries, aiming to erode their political sovereignty, by influencing policies. Unlike many critical observations trying to claim the Ukrainian case and states with Russian-speaking population generally represent a unique case, and it is irrelevant to the West, the preliminary investigations of this project suggests that this is **an erroneous understanding of the problem**.

### *REVIEWING THE HYBRID WAR CONCEPT*

The critics assume a hybrid war **goal** is to simply make a sympathetic population do as the aggressor wishes – **support its aggression or at least be neutral to it**. It is an **excessively simplistic view** about hybrid war. In fact, the population-centered aggression mechanism has a set of choices: i) **direct loyal ethnic group** do as it favors the aggressor, **in an obvious support of aggressor's preferred policy** (opt for military neutrality, closer ties with Russia); ii) **direct a critical segment of the population**, which may be inimical to the aggressor, **oppose a policy** that is disliked by the aggressor

[9] D. Minzarari, IPRE Policy Paper, December 2020.

(**challenge EU, NATO, United States**, the national government disliked by the aggressor); iii) **create deep social fissures inside a society**, inciting some **segments of the population to challenge or threaten other groups** (incite **separatism**, **religious or ethnical tensions**, **political polarization**).

At minimum, when such a crisis is instigated by the aggressor, **the target government is unable to effectively oppose the aggressor** in areas of the latter's primary interests or **does not have the resources** and **political will to do it**. Among other things, it will distract the target state from many **foreign policy priorities** – for instance, **the EU states will be paying less attention to Eastern Europe**, **which would be a strategic goal sought by Russia**. At maximum, the target population may either **rebel against the incumbent governmen**t (one, which the aggressor does not like) and **replace it violently or force it out through snap** or regular **elections**. The latter case may not even be completely covert, as the aggressor may be interested in making it clear to the new, incoming government that it came to power due to the external involvement. For instance, in 2019, a Russia-funded political party – **the Party of Socialists – took over all three branches of power in the Republic of Moldova**. It made final **a hybrid war victory of Russia in Moldova**, even though it was tactical, due to the presence of a strong and active opposition. As a result, though hybrid war the aggressor **may reverse policies, acquire ad-hoc or even full control over the new government**.

A second track of the hybrid war type of **conflict technology**[10] is exploited directly through **the political leadership** of the target country. This may happen via **economic incentives**[11], **financial enticements**[12] or certain **political pressure mechanisms**[13]. Provided the territorial gain is an interstate aggression goal of a lower frequency, comparing to the past[14], the preferred goals of modern interstate aggression are **influencing or changing policy**. This makes the proposed hybrid war approach focused **on population and political leadership quite appropriate**.

[10] By conflict "technology" or the technology of aggression, I 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, pp.773-792, a conflict technology takes the conflict efforts from the input, specifically processes them, to provide victory, draw, or defeat at the output.

[11] Consider energy projects, promises of investment opportunities, etc. In the Republic of Moldova this includes the ex-president's relatives having joint business ventures with people connected to the Kremlin. In Ukraine, for instance, Viktor Medvedchuk – an influential member of parliament – has family businesses in Russia.

[12] There is an increasing volume of data and research suggesting Russian money have been used to fund political parties and campaigns in UK. See, for instance, Ed Caesar, "The Chaotic Triumph of Arron Banks, the 'Bad Boy of Brexit,'" The New Yorker, 18 March 2019. https://www.newyorker.com/magazine/2019/03/25/the-chaotic-triumph-of-arron-banks-the-bad-boy-of-brexit

[13] It is not entirely clear what has led Harry van Bommel, a Socialist Party Dutch MP, to use Russian nationals and present them as "Ukrainians" in order to campaign in Netherlands against Ukraine. See Andrew Higgins, "Fake News, Fake Ukrainians: How a Group of Russians Tilted a Dutch Vote," New York Times, 16 February 2017. https://www.nytimes.com/2017/02/16/world/europe/russia-ukraine-fake-news-dutch-vote.html. More recently, media has been voicing the idea that Trump has been indirectly developed as a Soviet KGB asset since late 1970s. See D. Smith, "'The Perfect Target': Russia Cultivated Trump as Asset for 40 Years – ex-KGB spy," 29 January 2021.

[14] See Militarized Interstate Disputes data set of the Correlates of War Project, https://correlatesofwar.org/data-sets/MIDs.

### *OBSERVABLE IMPLICATIONS*

Having explained the hybrid war process, we are now interested in understanding what the observable **implications** of this **interstate aggression technology** are. In the case of **territorial military invasion**, we would look at **military exercises in geographic proximity**, **at troops mobilization**, at **the military deployments and amassment at the border, aerial reconnaissance overflies, or at the preparation of transportation routes,** like it happened before the 2008 Georgia-Russia war. For an early warning mechanism, we need to identify **a set of similar indicators**, which would be highly representative, either alone or in various combinations, of **a hybrid war initiation risk**. A significant handicap is that **we have a reduced volume of observations** in regard to the military indicators in a hybrid war. Ukraine had a Russian military base on its territory, which was used to consolidate the hybrid aggression gains against a possible recovery through military means by the Ukrainian authorities. A similar situation could be observed in the 1992 Republic of Moldova, where Russia used the military bases, it controlled in the **Transnistrian region to squeeze Moldovan authorities** (including the law enforcement) **out of the region and then coerce them into accepting Russian ceasefire terms**, in a way rather identical to the developments in Ukraine's Donbas. In fact, **the presence of Russian military forces on the territory of a potential target country, or in its proximity, is a static indicator of a hybrid war risk**, because it gives Russia easy access to capabilities allowing defending and enforcing a new status quo. Based on this, we are more likely to see the emergence of **effective separatist entities (protected militarily) in Eastern Europe**, **including Baltic States** – in proximity to Russia – **than in Western Europe**.

However, new data suggests that there are additional mechanisms that could lead to the emergence of Russia-backed separatist entities even in Western Europe, mostly through **proxy forces.** For instance, the Spanish authorities reportedly found about a possible offer, made by a Russian group to the **Catalan separatist leaders**, to **provide a few thousand soldiers**, apparently **for the protection of a new status quo** after independence declaration.[15] Over the last several years, media reported about **para-military training camps organized for far-right groups by Russian nationals** (or with Russian support) either on the Russian territory, or **in Europe** (**Slovakia, Hungary, Serbia, Bosnia and Herzegovina**).[16] There is a significant risk that such groups could be **used by Russia for operations in various countries in Europe**. Therefore, while the military aggression is not of primary concern in a hybrid war, **the military indicators**

[15] Politico.eu, "Russian Group Offered Catalan Separatist Leaders 10,000 Soldiers, Judge Says," 28 October 2020.
[16] See DW.com, "German Neo-Nazis Trained at Russian Camps: Report," 5 June 2020; M. Carpenter, "Russia is Co-opting Angry Young Men," The Atlantic, 29 August 2018; RFE/RL, "Serbian Police Close Paramilitary Youth Camp Run by Ultranationalists, Russian Group," 17 August 2018; or D. Salvo and S. De Leon, "Russia's Efforts to Destabilize Bosnia and Herzegovina," GMF Brief nr. 17, 2018.

**that reflect the indirect, proxy kind of armed involvement** to secure a newly established political status quo, should be considered.

Therefore, the goal of a theory-based early warning model addressing hybrid war is to look at the crossing of various threat thresholds, which would be in line with an **escalation logic**, suggested by the proposed hybrid war theory.[17] The analyst will be looking at the events in the information environment as reflecting developments in the interaction between the aggressor and the target state. These events will signal and be the evidence of the application of certain hybrid war tools and actions, similar to how concentric circles in the water reveal that the water surface at the center of the circles was exposed to a shock. Whenever we see these circles in the water, we know there was an impact with the water in the proximity. Because **specific events - like information operations (manipulation, disinformation, misinformation, etc.), in case they are not accidental but reveal an organized and massive-in-scale focus - suggest a particular political goal is pursued,** we should include them in our early warning matrix. A visual illustration of this logic is presented in figure 2.

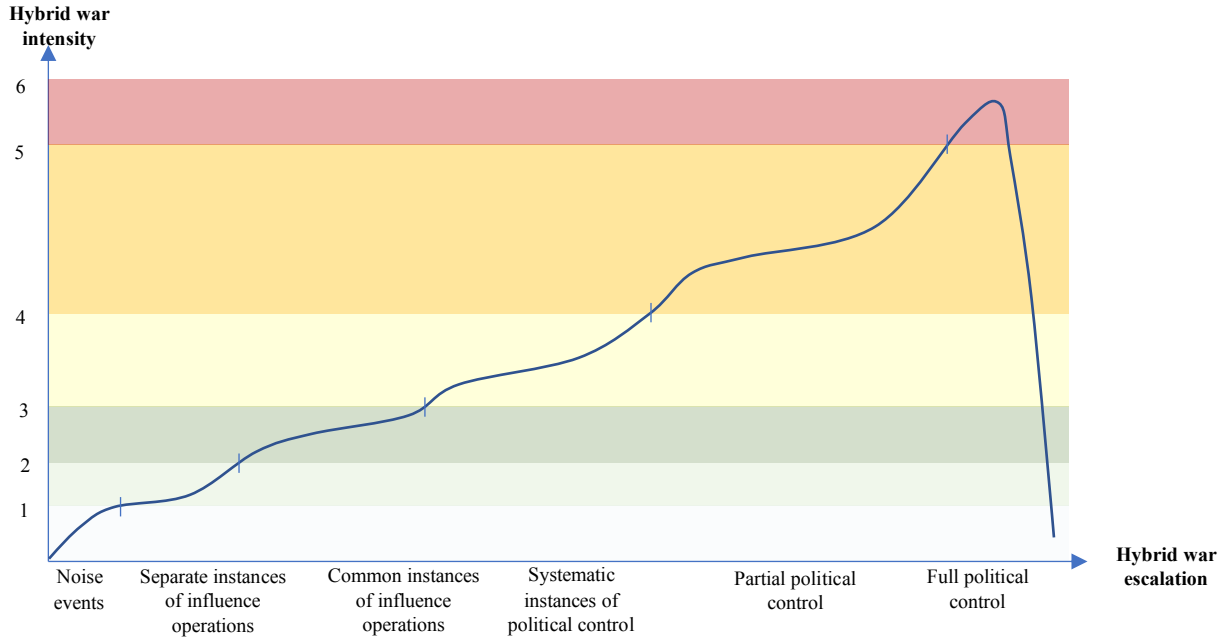



***Figure 2: Hybrid war intensity and escalation thresholds***

On its Y axis (fig.2), this model presents the hybrid war intensity in terms of its effects. On its X axis, it lays down the escalation steps of hybrid war, in terms of its related activities. Therefore, if we observe common instances of information operations targeting the domestic population or separate segments of it, pushing it towards certain actions or inactions, or aiming to alter their preferences, the model proposes a level-transition from a moderate threat level towards a substation one (fig. 3).

[17] D. Minzarari, IPRE Policy Paper, December 2020; see also D. Minzarari, NDC Policy Brief nr.19, November 2020.

| | | |
|---|---|---|
| 6<br>Extreme | Threat event triggered | Respond to and mitigate threat event effects |
| 5<br>High | Frequent occurrence | Carry out actions to manage risk |
| 4<br>Substantial | Systematic occurrence | Develop measures to lower risks |
| 3<br>Moderate | Common occurrence | Monitoring for connections among indicators |
| 2<br>Low | Rare occurrence | Monitoring |
| 1<br>Minimal | No changes | No action required |

***Figure 3: A risk-level assessment model***

In terms of policy responses, it demands switching from **a monitoring posture to a reaction one, deriving measures to address the risks triggered by this escalation**. In practical terms, this would mean reducing the entry channels for information proliferation, including **closing down media outlets and sources** that do not follow the **common codes of journalistic standards** and **ethics**.[18]

For more clarity, let us examine an example. The "partial political control" escalation level would be similar to **pre-invasion stage** in a conventional war setup, when the aggressor troops have amassed at the border and already started bombarding the defending troops of the target state, to prepare for crossing the border. In most Western countries this may be the apex of the confronted hybrid war effects, as to them losing control of one or two branches of political power, while extremely damaging, does not necessarily mean transitioning into the red, extreme threat zone. To states with **developing political systems** and with fragile state institutions, **losing control over one of the branches of power creates a significant likelihood of complete loss of sovereignty**, thus **transitioning into the red threat intensity zone**. For reference, most EU countries are in the moderate (dark green) zone, with a very few in the substantial (yellow) threat zone. Following its recent presidential elections, Moldova is in the high risk (orange) threat area. **After an aggressor takes full political control of the target state**, the evaluation of the new regime can be started from the beginning of the escalation cycle, as indicated on the graph.

The analyst conducting the early warning should have a solid understanding of the underlying hybrid war mechanism. This allows to attach accurately specific actions to the escalation or intensity stages. **It is impossible to provide a written description of all the actions, distributed across the stages, given they may take different shapes**

[18] See for an example DW.com, "Ukraine: Zelenskiy Bans Three Opposition TV Stations," 3 February 2021.

**and forms.** To facilitate the analysis, the focus should be on the **actions' effects,** and how they would map into the proposed model of hybrid war. Therefore, the analyst should understand well the expected effects of specific hybrid war actions. For instance, the acquisition of economic or business interests by a political figure, or any person with significant political influence, will likely make that figure vulnerable to the pressure of the actors that control the business or economic transaction. It shall be of no surprise that the former German chancellor Gerhard Schröder, after being hired by Russia's state-owned energy companies Rosneft and Gazprom, has the interest and ability to lobby for the Russian state interests in Germany.[19] Similarly, the acquisition by the brother of former Moldovan president Igor Dodon of business interests in Russia, and the consequent evidence that Dodon's Party of Socialists is funded by the Russian state, would qualify enacting the orange level of threat, at minimum.

The analyst effort in conducting early warning can be assisted by developing some umbrella categories, which aim to provide a general description of the impact of high-likelihood actions, mapping them on the hybrid war escalation ladder. To capture the proposed hybrid war model, these categories would have to relate to **the three targets of hybrid aggression: (1) population control, (2) political leadership control and (3) territorial control**. **Furthermore, they will be assessed along a set of structural categories**, which reflect the wider **field of conflict escalation studies**, but also are relevant to the three core categories. The proposed **structural categories** are as following: **(a) economic, (b) government effectiveness, (c) political stability, (d) security, and (e) regional affairs**. These categories have also been evaluated in terms of their **context suitability**, **to reflect Moldova's conditions**. For instance, a frequently examined category in conflict studies is the presence of **natural resources** (over which fighting may erupt) that **is irrelevant to Moldova's case**.

## 2. HYBRID WAR INDICATORS

The following table will present a set of indicators that is expected to assess the threat and its levels of risk, for the early warning against hybrid war activities (tab. 1). The economic, government effectiveness, and regional affairs indicators are contextual. They can persist for longer times, accumulate, and increase the level of risk, understood as the likelihood of harmful event occurring. They can trigger the threat event if able to accumulate sufficient pressure on the state resilience mechanism. However, the relevant threat event will be most visibly, but also directly produced by the political stability and the security indicators, which will act as triggers. The contextual indicators will serve as drivers for the trigger indicators and will suggest to the observer that the likelihood of emerging of trigger indicators will increase, as contextual indicators accumulate.

[19] DW.com, "Politicians in Germany Warn Ex-Chancellor Schroder to Quit Russian Posts," 6 September 2020.

| Contextual indicators | Target areas | | |
|---|---|---|---|
| | 1. Population | 2. Political leadership | 3. Territory |
| a. Economic | ***1. Inequality***: Quick or recent and sharp increase<br>***2. Shock***: economic shock or financial crisis (including those triggered by cyber-attacks)<br>***3. Unemployment*** rate<br>***4. Sanctions*** affecting groups of population<br>***5. Trade dependence*** impacting exports/critical imports | ***1. Dependence***: business interests<br>***2. Corruption*** charges and evidence against key leadership<br>***3. Removal*** of obstacle for foreign acquisition of strategic assets | ***1. Blockade***: of physical trade routs<br>***2. Calamity***: natural or technogenic, which impacts economic output<br>***3. Selective trade***: trade preference to specific region or group by a potential aggressor<br>***4. Self-governed (SG) areas trade*** with EU |
| b. Government effectiveness | ***1. Insecurity*** perception, based on specific threat – crime, ethnic targeting, coercion<br>***2. Legal*** selectivity: selective justice<br>***3. Corruption*** network affiliation | ***1. Capture*** of state institutions by specific party or interest group<br>***2. Independence*** from political pressure, either domestic or foreign<br>***3. Public support*** across the country | 1. Effective ***law enforcement*** in all regions<br>***2. Control*** of borders and entry points (airports, maritime ports, border crossing points)<br>***3. Tax collection*** across all territory (lack of access, locally or centrally collected taxes) |
| c. Political Stability | ***1. Protest frequency***: how often<br>***2. Protest geography***: how dispersed across the country<br>***3. Protest violence***<br>***4. Protest grievance***: paid or genuine participation<br>***5. Trust*** in government<br>***6. Trust*** in opposition<br>***7. Ethnic*** drivers | ***1. Ability to mobilize*** critical-mass protests<br>***2. Ability to attract*** and maintain Western ***support***<br>***3. Effective control*** of protests<br>***4. Information targeting*** of policies or politicians | ***1. Push for increased self-governance*** by ethnically homogeneous pro-Russian areas<br>***2. Unilateral political*** decisions of ethnical SG areas<br>***3. Informal and formal connections*** between ethnical SG areas |
| d. Security | ***1. Military exercises*** frequency of foreign(-controlled) troops<br>***2. Military training*** complexity | ***1. Frequency of*** foreign ***visits***<br>***2. Support*** of foreign ***military presence*** | ***1. Strange transportation links*** with aggressor's territory (Chisinau-Rostov) |

| | | | |
|---|---|---|---|
| | ***3. Frequency of incidents*** (*not exercises*) in the Security Zone<br>***4. Military trainings of civilians*** (non-state) | ***3***. ***Supply*** of foreign ***military presence***<br>***4***. ***Defense and security budgets*** support<br>***5***. ***Supporting military cooperation*** with aggressor's military | ***2. Air cargo*** to non-central airport (military, or "civil emergency")<br>***3. Non-alternative energy*** connections |
| **e. Regional affairs** | ***1***. ***Pushing for policies*** favored by aggressor<br>***2. Pushing against policies*** rejected by aggressor | ***1. Favoring regional initiatives*** led by aggressor<br>***2. Undermining regional initiatives*** balancing the aggressor | ***1. Decreased support*** of allies and partners<br>***2. Violation of international norms*** of sovereignty by the aggressor. |

***Table 1: Hybrid war indicators***

The evaluation of threat level (fig.3) is conducted by aligning indicators along the hybrid war escalation mechanism. Provided the hybrid war-related actions aim at influencing or controlling the target state policies, the analyst should identify where in the sequence of the hybrid war mechanism the observed event is placed. This way we can get the intuition whether we are likely at the beginning of a threat event build-up (green), the threat is in active phase (yellow), is in pre-trigger phase (orange), or has been triggered and is escalating (red). For instance, when former President of the Republic of Moldova, Igor Dodon, used his control over the Parliament to sack Maia Sandu's Government in 2019, this event was at the extreme, red risk level. The orange level emerged when Sandu was warned to roll back her reform actions focused on the general prosecutor office.

By conducting a usual level (dozens per year) of military exercises in the Transnistrian region – in line with pre-2014 patterns - Russia would support a minimal hybrid war risk level. Increasing the number of exercises and their content would move up the risk ladder to level 2 and even 3. Forcing the Moldovan peacekeepers to leave their positions would elevate the risk to substantial, while deploying additional troops to the Security Zone or outside, would make the threat risk to be high. This would be based on the understanding of how these troops are to be used, what is the goal of their deployment and what are the end points of the conducted actions.

As another illustrative example, the language-issue protests that the Party of Socialists organized across the country in early 2021 would be in the area of low to moderate (2-3) risk. Or, the establishment of an air transportation route between Chisinau and the Russian region of Rostov could actually signify a substantial risk (4), if additional indicators suggest this is done to bring military-trained personnel into Moldova. This, of course, is based on analyst's contextual knowledge that Russia opened training facilities

in its south-east Rostov and Krasnodar regions, to prepare armed groups for Donbas and Syria.[20]

The underlying logic is that we estimate – based on the previously-defined hybrid war model – what are the steps of hybrid war escalation. The EW model would then identify the indicators preceding these steps and suggest a crisis escalation level, based on their assessment. This is a more of **a predictive approach**, based on **model-defined features**, rather than **a forecasting one that is based on identification of similar trends in large amounts of data**. While the related **data-collection** efforts require limited **training** for the human operator, the **analysis and interpretation** of this data presents a high demand of **contextual and theoretical knowledge** from the involved analysts. However, the majority of the existing policy early warning models use human experts to conduct this exercise, mostly for the reasons listed earlier.

The quantitative measuring and analysis models have limited accuracy and employ various aggregation, weighting, and probabilistic technics. Some explore the frequency of various violent and nonviolent incidents and their interaction, some apply aggregation techniques to structural socio-economic indicators, and others explore correlation links between the risk of conflict and selected structural indicators.[21] To conduct a similar exercise for a hybrid war type of conflict technology, one would need lengthy data collection efforts, tailored to this type of conflict dynamics. A parsimonious theory of hybrid war would be required, or of a conflict type that reveals similar traits. This project, to the knowledge of the author, is the first one to propose such a theory. Provided the project will trigger a data-collection effort that is technically accurate, tractable, systematic and continuous, it may be possible then to similarly design quantitative models that do not require the human operator involvement in the analysis and interpretation stages. A data collection exercise, based on a specific hybrid war model and its respective indicators, is possible for the Ukrainian case, given the history of that conflict. However, this would require effort and resources that are beyond the scope of this exercise.

## 3. THE STRUCTURE OF THE EW MECHANISM

The general process is straightforward and involves information monitoring and observation, information collection and logging into a database, information analysis to understand which phase of the hybrid war mechanism the observed event would likely belong to, and finally – the interpretation of the significance of the event. Schematically, the EW mechanism is displayed in figure 4.

[20] See Znak.com, "Врут все, сынок, они нефть делят! На крови ребят зарабатывают," 5 March 2018; BBC.com, " Сирия, Африка, Украина. Куда и как "ЧВК Вагнера" вербует людей и где их поминает," 23 November 2018; Rus.lb.ua, "СБУ узнала о 195 тренировочных лагерях боевиков 'ДНР-ЛНР'," 28 August 2015.
[21] C. Burnley, D. Buda and F. Kayitakire, "Quantitative Global Model for Armed Conflict Assessment," JRC Scientific and Technical Reports, 2008, p.5.

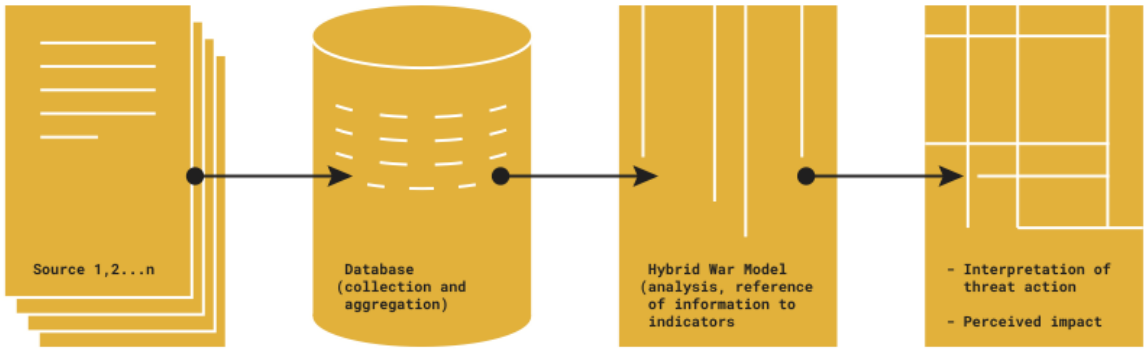



***Figure 4: The early warning mechanism (schematic diagram)***

The collection and logging of data is done based on the earlier-listed indicators (tab.1), and it should include (as an example)[22] the following information, collected across determined time segments:

1. Type of event (can be referenced as 112, or 323, etc., where the first digit represents the type of indicator, the second digit represents the target of the hybrid war attack (population, leadership or territory), and the third digit represents the indicator at the intersection of the first two categories;
2. Date and location of event (the date allows for the evaluation of temporal distribution of events and same-event clusters, while the location allows to visualize them on the map and identify geographic patterns);
3. Benefiting actor (who gains);
4. Agency actor (who drives the action);
5. Quantity of events/frequency/intensity.

The Ministry of Economy and Infrastructure may not be interested in military exercises, which would mean they would focus on selected indicators of interest. Intelligence agencies may be interested in the whole range of indicators, unlike the Ministry of Interior, or the Ministry of Justice. Civil society observers that would like to use the model, could also adapt it to their needs – a social issues focused NGO won't look into military exercises either, or may adjust the model to account for forcefully-recruited or illegally arrested people in the Transnistrian region.

[22] The analyst or the EW process manager may decide to include additional data types, if they allow for a better reflection of the impact of the EW indicator.

In the simplest application, the data is collected in a MS Excel file, which also allows conducting a large variety of analytic exercises and visualizations. The risk level is to be added following the last stage – the interpretation of threat action.

This approach requires continuity in data collection and maintaining a solid contextual knowledge about the issue area. The more data becomes available, the sooner we are able to automatize the process of analysis, acquire the ability to identify and understand patterns in data, and improve the accuracy of the analysis. As emphasized earlier, the contextual knowledge of the analyst is useful at the initial stage (12-24 months), when there is little data, and when making sense of events would require background knowledge about both methods and the conflict environment.

The knowledge of conflict models, including the employed theory of hybrid war, is another important requirement to the analyst. For instance, they will help understand and identify the set of conditions that may typically precede the outbreak of hybrid conflict, while not being present in cases when the conflict is not likely triggered. At the beginning, it will also be useful to monitor for the possibility of patterns and process-dependent aggregations of indicators. Or, the joint occurrence of exercises, the deployments of forces to the administrative line with the Transnistrian region, the protests in specific regions and potential transportation of personnel from Russia would cumulatively indicate an orange-to-red risk level of the hybrid war threat. The frequency and intensity of events is a referential notion for this model and should be measured in comparison to a previous mean value. This would allow to identify deviations from the past “normal”.

In a way, this theory-based EW mechanism has an analytic similarity to the process followed by an international affairs or country expert, although is tailored to the hybrid war model developed in the earlier stages of this project. As the data is being collected and analyzed, this would allow to verify empirically the explored hybrid war model and improve it through a feedback loop. Nevertheless, this effort will be affected by missing data bias, as it will be vulnerable to media coverage omissions, which may intentionally under-report events, or miss them altogether. Intelligence agencies will be able to partially compensate for this, being able to fill in the database with information flows from closed source intelligence.

## 4. Early Warning Algorithm

### *Data Collection*

The EW mechanism starting point is *data collection* and its logging into a database. For general purpose data collection, the operator will identify a number of media sources, both national and foreign. The sources need to be trustworthy, known for their journalistic standards and ethics. We would need a few, so that we can cross-reference events of interests for details – some may have the wrong time or figures, others might have gotten

the facts not completely covered or covered with some errors. A subject matter (political risk, intelligence, conflict analysis) expert will be able to spot, frequently, these questionable details and seek verification through alternative sources.

Online written sources are most convenient and time saving. The operators would select their preferred and most trusted local outlets, which need to be news intensive. Some examples are stiri.md, unimedia.md, realitatea.md, newsmaker.md. Provided the weight of political (ethnic) polarization indicators, it is necessary to follow local news from Transnistrian region, ATU Gagauzia and Balti. The operators will select their sources (two independent-of-each-other would suffice) for verification purposes. Additionally, the operator should follow a few Russian sources, including the Ministry of Defense, mil.ru, (for data on exercises in Transnistria, or troops rotations, equipment updates, etc.) – and others like ng.ru, mk.ru, topwar.ru, which can be verified on a weekly basis, through general or website searchers. The frequency of local (Moldova) data collection should be on a daily basis.

Data should be collected based on the events that reflect conceptually the listed indicators. Some indicators may get flagged and logged in frequently, while others only on rare occasions. For instance, it is unlikely to have protests every week or even every month. For such indicators it will take some observation time until the operator can make informed estimations linked to these indicators. If we are interested in the ability of a party or group to mobilize critical-mass protests, or large protests for Moldova, historical data will have to be researched. This may be required in case the analyst has a number of indicators active and would need to verify if an involved party has the capacity for protest mobilization, in order to assess whether the current data will place the risk at a lower or more elevated level. In this sense, the EW assessment will be an interactive process with the researched environment.

### *Assessment of indicators*

Indicators like unemployment rate are only periodically updated by the governmental institutions. The operators will have to flag the new data release dates, if these are fixed and update the database accordingly. A similar approach is suggested for any type of periodically issued data. Other data, like population perceptions about political parties and forces, will be also issued periodically, based on targeted population surveys. The operators need to account for the fact that most surveys in Moldova are manipulative and paid by political parties to influence and direct public opinion. In this case, one of the possible approaches is to do an averaging of the data of interest across a few surveys and use more trustworthy ones (i.e. IRI) as a benchmark. The operator should keep in mind that most of the data provided by international or intergovernmental organization has significant bias in it, as it is provided by the governmental statistical service or is based on questioning of groups that have vested interests in these surveys. For Moldova,

the statistical data from its official governmental body has not been known for being manipulated, but the operator should keep that risk in mind.

Some indicators will have to be accounted by the operator based on the news analysis. For instance, the "capture of state institutions" indicator would rarely be objectively mentioned in the media. However, the media will give the pieces of the puzzle that the analyst will have to put together. If a political party or group that is known for having interests, dependencies, or other similar connections to Russia, has managed to acquire control over a ministry, governmental agency or branch of state power, the analyst would have to consider this development towards the respective indicator. Russia for now is the only country, which is known to systematically work towards undermining Moldova's sovereignty. This assessment should also be issue-specific – a negative event in terms of state capture will only occur if the agent of interest is linked to a foreign country who has policies that go against Moldova's policies. Because the Republic of Moldova chose as its strategic priority to develop closer relationships with the European Union, and potential accession to the EU, a political party, group or politician that is believed to be EU-sympathetic will not trigger a negative event. In this example the two interest – the state one and that of the political entity – converge. Another instance of state capture may occur if a local actor takes control over governmental institutions for advancing private interests – the case of Vladimir Plahotniuc is an example. The operator may distinguish in its data logging the domestic or the foreign state capture. It is impossible, given the limited scope of this project, to go over every single indicator, as this may require extensive space. The analyst should use her knowledge of the hybrid war model, her subject-matter training and common sense to match the observed data with the indicators from the EW matrix (tab.1).

A simplest yet effective approach is to use an MS Excel file for *logging the data*. It will have to be logged based on the data categories of interest. An example was offered in the previous section, using the five data inputs: type of event, data and location of event, actors involved, quantity of frequency. This is an example, which can be extended with more data inputs, depending on the analytic demand of the particular agency/actor that runs the EW.

| **Indicators** | **Data traits** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | ***Day*** | ***Loc*** | ***Freq*** | ***Actor1*** | ***Actor2*** | ***Size*** | ***Intensity*** | ***Funds, $*** |
| **411 (or MilEx)** | 11Feb | Sangera | 2 | Russia | Trn | Small (platoon) | CPX | N/A |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **MilEx** | 4 Mar | Tighina | 1 | N/A | Trn | Medium (comp) | LFX, FTX | N/A |
| **112 (or Dpnd)** | 10 Mar | Chisinau | 1 | PSRM | Russia | N/A | N/A | 50,000 |
| **Inflation** | 10 Mar | RM | 1 | Population | Gov | N/A | 5% | N/A |

***Table 2: Data logging example***

The table above, which will be an MS Excel file, reveals the flexibility of the operator – it has it while initially building the indicator characteristics or traits, although it will have to stick to them, following that. Eventually, the operator may realize a different trait might be better at describing the indicator. Then a new column can be added, and the new trait would be monitored from that time on. Ideally, the operator will also research the past missing data for this new trait.

The table reveals the importance of subject and contextual expertise of the operator and or the analyst that identified the traits. For instance, depending on interest, military exercises can be qualified as command post type (CPX), live-fire exercises (LFX) or field training exercise (FTX). The sizes vary, but in Moldova's Transnistrian region the exercises are conducted usually at squad/platoon, company, or battalion/brigade levels. Again, the subject matter expert will evaluate what are the typical sizes and adjust the inputted data accordingly, as consistent notation is critical. The operator/analyst can get creative and if they don't have a specific notation. For instance, if they want to mention that the platoon-size exercise involved two platoons (one infantry and another artillery), they can add an extra column to mark this now and in the future. The operator can use either the number code, or the abbreviated indicator, though it has to be consistent.

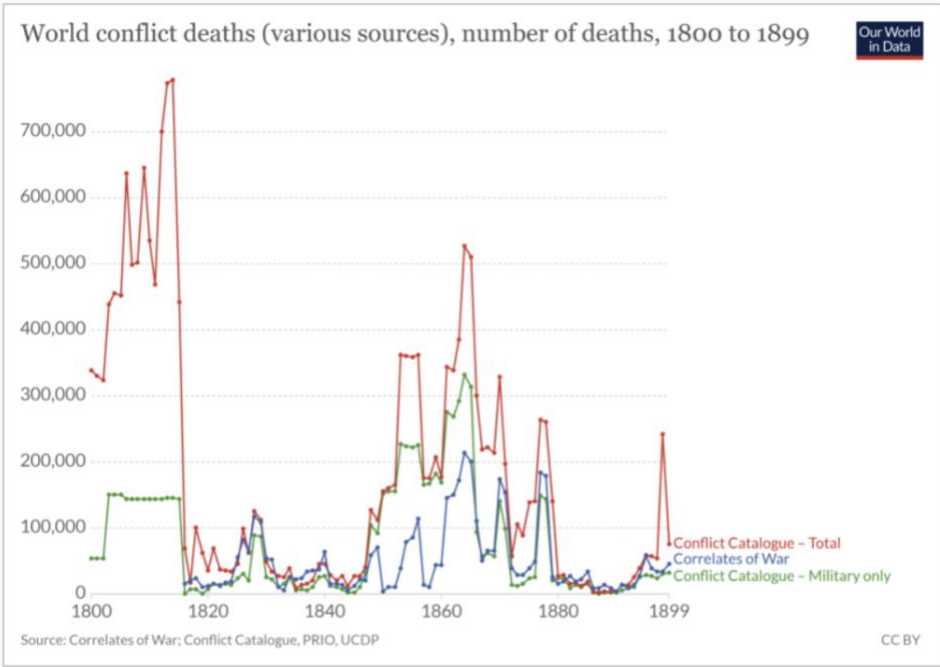
Let's try an example of another indicator – "dependence: business interests" or 112. That row indicates a hypothetical incident of PSRM receiving $50,000 from Russia on March 10, in Chisinau. Similarly, we could record the news about ex-president Dodon brother entering a joint business venture with the son of Yuriy Chayka, with strong connections to the Russian government. We could add a new trait column if none of the existing ones would logically capture any important detail, which we would like to log in on a systematic basis. Some indicators, like inequality, are difficult to directly collect data on. In this case, the analyst would consider which indicators could be combined to offer information that are giving us a systematic understanding of inequality indicator. I suggested inflation, and the last row indicates an example value of inflation as reported on 10 March. An economist would identify 2-3 (preferably no more) indicators that would be informative of economic inequality in Moldova. It is possible that this measure is reported regularly by the governmental statistics office, which will be then used. The conflict studies suggest

that a growing inequality is a strong indicator of violent conflict emergence. However, an economics expert may conclude that in Moldova there may be a different indicator, reflecting more accurately the process of dissatisfaction with economic welfare among the poorest segment of the society. It would be useful such suggestions to be shared across governmental agencies, so that there is a horizontal consistency in data collection. Depending on costs and resources, agencies may decide to distribute data collection among them and then share the results. Or, they may collect the same data separately. There are tradeoffs in either of the cases.

### *DATA ANALYSIS*

The *data analysis* process may take different forms, depending on the needs and resources of the analyzing actor. MS Excel provides a range of analytic tools, of which the most relevant will be observing variation of a specific indicator across time, alone or contrasting with another indicator. For instance, below is a graph illustrating how we can combine related type of data from three different sources (fig.5). This would be similar to three indicators of interest from our EW matrix, that may interact in some way – i.e. either amplify a variable of interest or diminish its effects. Or, the analyst may conduct exploratory analysis and graph different indicators to examine how they might correlate over time.

Geographic locations from Excel can be exported into *GoogleEarth* and examine the existence of geographic patterns. To achieve this, instead (or together with) the location name, the operator may include the geographic coordinates, as well, in a separate column. This would be particular useful for indicators reflecting protests, military exercises, incidents of corruption, economic indicators of inequality per region, etc.




Graph of global conflict deaths from 1800 to 1899 from various sources.

***Figure 5: Graphing of three time-dependent variables (example).***

### *INTERPRETATION AND IMPACT ASSESSMENT*

At the *interpretation and impact assessment* stage the analyst would have to rely on the conclusion from the data analysis. The analyst will then map analysis results on the hybrid war escalation scale, considering the hybrid war model. The emergence of some of the security and political stability indicators would clearly put the risk at the orange or red level – the taking over 1-2 or all three of the branches of power was one of the examples. Some of these would be indirectly deduced from the contextual indicators – for instance the expected win of a party in elections. However, most of the indicators would allow us to map the risk level in the green and yellow areas. It is not possible to derive a more numerical approach. We don't know whether a 5,000-large protest for one day may trigger a government to resign or if this would be triggered by a 500-large protest during a month. However, this EW mechanism is not tailored towards micro-events, like a government resigning. It instead focusses on macro-events like partial or complete loss of political sovereignty, for which a higher accuracy and a longer anticipatory time length are possible. It will also allow, with the accumulation of data, to identify patterns of unrelated data and indicators' interactions that have useful prediction purpose.

At this stage, though, the interpretation and assessment is driven mostly by the subject expert analyst. For instance, the data would allow the analyst to see the frequency of military exercises. Based on their types and complexity the analyst would be able to derive

what is the purpose of the exercise. In addition to this, by putting together information about exercises, worsening economic indicators, negative variations in trade of SG areas with EU, blockades, possible protests, etc., the analyst would be able to elevate the hybrid war threat level, given an explosive mix of indicators. In turn, this information would be useful for authorities as they would know where to focus and which indicators to address for de-escalation or deterrence.

The legislation allowing the foreign acquisition of strategic assets would serve as another red flag for the analyst. Given the data collected across other indicators, the analyst will be able to look how this incident correlates with other related indicators. He would then explore correlations and look to test and verify causal mechanisms explaining the reason for this decision being advanced at this point in time. It could be possible that only the economic indicators won't be useful. At this point the analyst would look across other structural categories of indicators. This stage of the EW mechanism is more similar to a quest, where the analyst explores the power of aggregated data, of having a selected set of indicators – related to the hybrid war model – being brought together. The analysis is useful to conduct on a weekly basis, unless a triggering type of indicator is being recorded. At the initial stage, while the data is being accumulated, the analysis would be more of an exploratory nature. After a longer history of data is gathered, the weekly analysis exercises are expected to become more meaningful, as trends and correlations will emerge more clearly.

## TOWARDS AN EW MECHANISM FOR THE REPUBLIC OF MOLDOVA

### *CONCLUSIONS*

Moldovan actors – either governmental or NGOs – have not historically conducted any systematic EW risk assessment or exercises. Due to this reason, there is little EW designated data, in addition to the regular data collected by governmental statistical office. This makes the initiation of an EW mechanism, in particular covering the specific threat of hybrid war, an uncharted territory. It also means that the are no designated resources, structures, training, and effort ready to start its implementation. Technically, there are a few ways to implement a hybrid war EW mechanism in Moldova.

One way would be to distribute the indicators across a few state institutions and allow them the liberty to adjust some or include new indicators, in line with the hybrid war model. The institutions would mostly conduct data collection, logging in, and analysis of their indicators. Then, they will send the logged data and analysis on a regular basis (weekly or monthly) to an agency that leads the national effort on countering hybrid threats. That agency would aggregate the data and let its analysts examine both the raw data and the analytic inputs received from the partner agencies. This would bring a number of benefits, in particular would allow more than one institution to develop EW domain-specific capabilities, both at the monitoring, data aggregation and analytic levels. The downside is that it will require more resources to be invested. It is important, however, for certain governmental institutions to have their EW cells – the ministry of economy, finance, social protection, health (pandemic threat), civil protection, interior, defense, and the intelligence service, among others. They will greatly assist these institutions in their planning process and in optimally directing their scarce resources towards the most critical areas.

However, as this paper revealed, implementing, maintaining, and consequently developing a hybrid war early warning mechanism is a labor-intensive activity. It demands that considerable resources and highly skilled personnel are tasked with this on a permanent basis. Daily data monitoring of several media outlets, as well as other sources of information, demands a dedicated team of data operators. Logging in the data in accordance with the indicators is another time-consuming permanent task, which also requires a tight interaction with the analysts. It is possible to have the same personnel conduct the data collection and analysis, but these are two different skill sets, with the latter being considerably more technical. It is also a quite time-consuming one.

Consequently, a constructive setup would demand at least two specialized teams: one for data collection, and another one for data analysis and interpretation. While in Western countries this may not be a problem, in Moldova it could be a great challenge, given that whole departments in some ministries might have less than ten people. Another challenge

would be incorporating information from closed, classified sources into the model and analysis.

Finally, given the changing political situation in Moldova it is not clear for now which institution should be designated as leading the national effort to counter hybrid threats on the operational level and thus managing the EW mechanism. It could be the Security and Intelligence Service (SIS), or the Presidential Administration – the Security Council. In the former case, the nature of SIS may reduce productive interagency engagement due to its secretive nature and protocols. In the latter case, there may be insufficient protection of information with likely data leaks. Adjustments need to be made in both cases – perhaps to relax the existing security protocols on this specific EW exercise in the former case and consolidate information security and access protocols in the latter case.

A parallel hybrid war EW mechanism may be implemented by the civil society, but it will likely be more affected by missing data bias, lack of resources to conduct the complete range of data collection and analysis, and reduced accuracy due to desegregation across the structural categories.

The latter will likely be due to specialization of existing NGOs, and lack of experts to cover all categories. However, given consistency and continuity, the civil society's effort to conduct this exercise in parallel with the governmental agencies, even if only on selected categories, will be useful.

The most important effect will be the watchdog one, as it may push the governmental agencies be more active and avoid ignoring certain incidents and developments. In particular, the most at-risk areas are related to corruption, state institutions capture by foreign or domestic actors, or the vulnerability in the economics and security areas.

### *Recommendations for Action*

1. Moldovan authorities should start discussions and designate a leading actor/agency for the national efforts to counter hybrid threats and activities (most suitable from the point of view of this author are SIS or the Presidential Administration).
2. A budget should be identified for funding personnel (10-12 people), facility, technical support, and training, to create a national EW Center; the benefit is that it could monitor, in addition to listed hybrid war indicators, some additional ones, including health/pandemic related, etc; a potential approach would be pooling funding form a number of interested governmental institutions.
3. Particular attention needs to be paid to the data protection and security of information and communication related to the project.
4. A clear algorithm for inter-agency cooperation, duties and responsibilities needs to be established, backed with specific legal framework.
5. A more effective information collection requirement system, at the strategic level and down to the agencies needs to be designed and implemented; Moldovan authorities need to depart from the current practice of ad-hoc decision making, heuristic solutions, and ignoring the added value of thoroughly informed decisions.
6. Additional resources and capabilities need to be established, built and operationalized in order to improve the data collection from closed sources; this should empower and support SIS and the Military Intelligence Department in conducting operational activities.
7. The MFAEI should be tasked to systematize its information collection and aggregation capabilities using diplomatic personnel abroad and domestically.
8. The Reintegration Bureau should be offered support to create an in-house information monitoring and analysis cell, given that a considerable part of hybrid war dynamics relates to the Transnistrian conflict and processes surrounding it.
9. All other governmental agencies should be tasked to design systematic information collection and logging efforts, related to their area of activity, addressing indicators valuable for strategic planning and forecasting (in addition to those related to hybrid war and their domain); ad-hoc practices should be stopped; the ability to conduct effective data-driven planning and forecasting will prove valuable at the stage of designing early response actions to hybrid threats.

## 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.


IPRE
Institute for European Policies and Reforms
ipre.md

Adress: str. București 90, of. 20,
mun. Chișinău, MD-2001,
Republica Moldova
Telephone: + 373 22 788 989
Email: info@ipre.md
Webpage: www.ipre.md