March 2021

Inside the “Bear Hug”: Fostering Resilience in the Belarusian and Ukrainian Security Sectors

Pavel Hanchuk

ReThink.CEE Fellowship
Summary

With the ongoing drastic transformation of the European security environment, problems of national resilience against hybrid destructive activity occupy a major place in policymaking at the state and international levels. This paper looks at how to foster the capacities of the security sectors of Eastern European countries to withstand the newly emerged combination of threats emanating from Russia. Its assertive actions that have already led to territorial and human losses represent a serious challenge to state sovereignty and societal well-being. The issue is vital especially for the Eastern European countries that constitute the front line of resistance to Russia’s malign activity.

This paper looks at two very close and yet considerably different countries—Belarus and Ukraine—to illustrate the challenges of adapting to a volatile geopolitical environment. It presents a comparative overview of transformations in their security sectors in response to Russia’s hybrid activities since 2014. It also reveals the main drawbacks in the security policies of Belarus and Ukraine in response to the changed security landscape.

In particular, Ukraine still struggles to overcome the limitations of its oligarch- and clan-based power structure, corruption, and the economic repercussions from conflict with Russia that impede smooth transformation processes. Despite being vocal regarding the priority of the security sector reform, since 2014 the country’s leadership has made little progress in reforming its intelligence sector, establishing an effective territorial defense, and enhancing strategic communications abroad.

At the same time, despite increased integration pressure from Russia, Belarus has moved more in the direction of securing the political regime rather than developing the whole-of-society approach to security required to counter hybrid activity. The clear divide between the state and society deepened further with the insufficient state reaction to the coronavirus pandemic and a new wave of repression against civil society linked to the 2020 presidential election. This exposed additional vulnerabilities that may be exploited by Russia to strengthen control over the regime.

This paper suggests a three-component capacity framework to enhance national resilience against hybrid activity. It introduces the notion of national cohesion, reflecting the convergence of the state apparatus and society’s interests as well as the ability of the population to influence national policymaking. In conclusion, the paper provides recommendations to national and international actors on possible ways to improve the awareness, coordination, and resource capacity of Belarus and Ukraine to better counter challenges coming from the east.
Introduction
The anti-hybrid narrative of Western policymakers and experts often neglects the frontline of resistance against Russian malign activities in Eastern Europe. While depicting the concept of hybrid threats in a thorough manner, it provides recommendations for societies where policymaking is deeply rooted in the principles of institutional checks and balances and the rule of law. As a result, practical initiatives that are relevant for NATO and European Union countries may not be fully applicable for Eastern European states operating in different political and security environments. These countries are usually constrained by corruption, the absence of transparency, and the lack of a vibrant civil society and properly functioning democratic mechanisms in general.

In Western countries, due to the well-established process of the replacement of elites through the ballot box, the level of cohesion between state and society remains relatively high. In addition, united in common intergovernmental organizations such as the EU and NATO, these states have deep resource pools at their disposal. These factors result in more transparent, receptive, and inclusive institutional setups that provide a basis conducive to an effective security policy to counter hybrid activity. The situations in states such as Belarus and Ukraine, however, are at best analyzed through problematic scenarios that have already happened, without formulating realistic policy remedies against Russian hybrid activity. However, the neutralization of hybrid threats requires the transatlantic community to act in a preventive manner. This includes fostering resilience in non-NATO neighboring countries that play an important role in common European security.

On that basis, studying the specifics of the security sectors in Belarus and Ukraine, including problems they face in their transformation from their post-Soviet heritage, is fundamental to building a solid belt of stability in Eastern Europe. This paper adopts a broad understanding of the security sector in which not only security providers but also national leadership and oversight structures play a role. They are usually represented by the government, the parliament, civil society, and the media.

In this context, the primary importance of Belarus for Europe and the United States is that it stays free from a serious Russian military presence, which would inevitably threaten not only Ukraine but also NATO’s eastern flank. As to Ukraine, the acceleration of post-Maidan reforms is crucial to overcome the fragility of the security sector that inevitably arises during a transition period. In fact, swift and effective policy measures are urgently required for Ukraine as the primary victim of Russia’s aggression and Belarus as it is largely exposed to the Kremlin’s influence in a way that directly endangers its sovereignty.

This paper presents an analysis of the hybrid threats from Russia targeted at Belarus and Ukraine, an assessment of the security-sector transformation in both states in the context of a changing security environment, and recommendations for building better resilience against hybridity in both countries.

Operationalizing hybrid threats
Security planning requires the operationalization of the concept of hybrid threats as its traditionally vague interpretation has little value for practitioners. In current research, hybrid threats are interpreted as coordinated hostile activities undertaken by an opposing actor, usually below the threshold of conventional warfare, in order to achieve certain goals. In most cases, such acts of interference aim to sow discord within the target society and to prepare the ground for further manipulation without substantially raising the threat perception of the object of influence. These activities are mainly grouped into overlapping phases of “priming, destabilization, and coercion.” Taking

---

into account their long-term character, hybrid activities usually follow a spiral-based model and their impact amplifies with time.

In addition, the tactics of destabilization do not have a standard blueprint when it comes to the set of instruments and their relative weight in an operation. Russia extensively capitalizes on an available infrastructure that includes legal frameworks, military facilities, networks of NGOs, agents of influence, and controlled media channels. In addition, it pursues different objectives depending on the country targeted, which ultimately determines the configuration of the hybrid toolkit.

On that basis, effective counter-hybrid policy planning has to start with a clear understanding of the opponent’s objectives. The main strategic goal of Russia’s assertive foreign policy in the post-Soviet space is to strengthen its domination over territories by exercising diverse forms of geopolitical control. These forms are primarily economic (energy supplies and integration projects), military (technological and numerical superiority), informational (propaganda and disinformation), and civilizational (appropriation of the Soviet heritage and promotion of the “Russian world” concept).

The primary reason fueling Russia’s hegemonic intentions is the protection of its regime. According to the worldview of the Russian political elites, shrinking control over neighboring territories presents an existential threat for the regime. Under this logic, Western actors aim to use any power vacuum to promote their interests and institutions there, and in the long term move NATO’s military infrastructure closer to Russia.

Russia’s Post-Maidan Strategy
Overall, Russian strategy in relation to the post-Soviet countries has been set to reflect the geopolitical reality in Eastern Europe formed after Ukraine’s 2014 Maidan revolution. Since Ukraine has stated that integration with Euro-Atlantic structures is its main foreign policy goal, Russia—having missed the momentum to tie the country to its sphere of influence—concentrates on discrediting its pro-democracy movement, reforms, and public authorities. In the case of Belarus, Russia mainly focuses on the erosion of sovereignty by pulling the country further into unequal and asymmetrical integration projects such as the Union State Treaty, the Eurasian Economic Union and the Collective Security Treaty; limits Belarusian strategic autonomy; and extends control over its economic assets. Generally, the common point of all Russian endeavors with regard to Belarus and Ukraine is to undermine state functionality and legitimacy.

In the pursuit of its objectives, Russia skillfully exploits the vulnerabilities of each country. Primarily, it benefits from the low level of convergence between state and society, and the malfunctioning of mechanisms of civilian control over public authorities. It widely uses these to expand the divide between actors within the country and maintain a state of controlled chaos there by undermining national cohesion.

Russia has followed this strategy during the upheaval in Belarus after the 2020 presidential election. It extended its support to President Alexander Lukashenko after his disputed reelection by providing security guarantees to quell the protests, allocating
additional financial resources to save the Belarusian leadership from economic collapse and sending propaganda specialists to assist pro-government media outlets. By backing the weakened autocratic regime, Moscow has sought political and economic concessions that Lukashenko would be willing to provide in exchange.

**The main impediment to developing societal resilience lays in the relatively weak sense of national identity.**

In Ukraine, Russia has capitalized on the state-society divide by discrediting transformation processes and magnifying the picture of related economic problems. The ultimate goals of such endeavors are to undermine the chosen development trajectory of Ukrainian society, destabilize the internal political situation, and promote Russian interests in the country.

The main impediment to developing societal resilience lays in the relatively weak sense of national identity, particularly in Belarus. Being constrained by an authoritarian state framework for more than 20 years, Belarusians have not formed a clear national identity, which has resulted in difficulties in reaching societal agreement on the perception of threats and the measures needed to repel them. In addition, the majority of the population supports close relations with Russia and speaks Russian.

Although the large-scale protests in 2020 marked the start of a national awakening, the rhetoric of pro-Russian societal consciousness and an as-yet underdeveloped civil society provide a weak base for national mobilization. In particular, the majority of security officials is largely susceptible to Russian propaganda and perceives the West as the main enemy. Overall, together with a critical dependence on the Russian economy (which accounts for almost half of Belarusian exports), Russia possesses a substantial base for manipulation and coercion in Belarus.

In the case of Ukraine, however, there is wide societal support for European integration and the majority of Ukrainians perceive Russia as an aggressor. At the same time, a large part of the population, fluctuating between 40 percent and 70 percent between 2014 and 2020, considers that the internal situation is evolving in the wrong direction.

Against this backdrop, most experts agree that the major weaknesses that contributed to Russia's operational success in 2014 are still relevant today in Ukraine. Among the main problems forming a background conducive to hybrid interventions are corruption and, linked to it, an oligarch-based economic system, mismanagement in the state apparatus, and the lack of training, modern equipment, and financial resources for the security sector. All these factors hamper the smooth and effective realization of the reform agenda and are aggravated by a growing fatigue with economic decline, thus making the Ukrainian state vulnerable to subversive activities.

**Undermining Sovereignty**

Russia’s actions in relation to Belarus have crystallized into a creeping effort at achieving submission by

---

3. Reuters, “Russia has agreed to lend Belarus $1.5 billion, Putin says at talks with Lukashenko,” September 14, 2020.

4. Institute of Sociology of the National Academy of Sciences of Belarus, “Half of Belarusians are not for allied, but for partner relations with Russia,” [original in Russian], December 12, 2019.


8. Liga BusinessInform, “63 percent of Ukrainians are convinced that the country is moving wrong – infographics,” [original in Ukrainian], July 2, 2020.

limiting the country’s autonomy in foreign, economic, and security policy. After having become a member of the Eurasian Economic Union (EEU) in 2014, Belarus lost its sovereign right to enter free-trade agreements with other states and organizations, which falls within the competence of the EEU institutions. Since 2016 Moscow has been pressuring Belarus to host new Russian military facilities and complete the formation of a joint military organization. Even though Lukashenko has managed to resist these requests until now, they clearly indicate that Russia is determined to reshape the format of the military alliance with Belarus by dictating its own conditions. In 2018, Russia’s Prime Minister Dmitry Medvedev issued an ultimatum to Belarus to fully realize the 1999 Union State Treaty between the two countries in exchange for the continuation of economic support. Among other things, this would entail the unification of their tax systems, the introduction of a single currency, and the creation of supranational institutions. Bearing in mind that there are no reasons to expect that Russia is interested in implementing treaty provisions on equal terms, such asymmetric integration would lead to the loss of the remaining sovereignty of the Belarusian state.

Despite facing a common threat from Russia, Belarus and Ukraine operate in structurally different security environments.

As for Ukraine, Russia conducts a range of activities to impede its rapprochement with the Euro-Atlantic structures. Keeping the country away from NATO’s military infrastructure and blocking its integration with the EU have been the main goals driving Russian actions since 2014. Russia therefore maintains tensions in Donbas and prevents Ukraine from joining NATO by preserving a “frozen conflict” in its territory. In addition, it undertakes measures to complicate any future reintegration of the territories it controls in Donbas. That includes issuing Russian passports to locals and substantially increasing state-sponsored propaganda in these areas. Russian disinformation does not target only the Ukrainian population; it also seeks to undermine the image of the Ukrainian state in the eyes of its main financial donors—the United States and the EU. Many experts say that the Ukrainian authorities have not reacted sufficiently to information warfare, despite it blacklisting Russian media outlets. This includes a clear gap in terms of security actors’ participation in information counter-operations and the lack of noticeable Ukrainian public diplomacy worldwide. In fact, disinformation is largely tackled by the international partners of Ukraine.

Russia continues the modernization and expansion of its military infrastructure along its borders with Belarus and Ukraine as well as in annexed Crimea. Since 2014 the number of Russian military personnel deployed in these territories has more than doubled. In 2020 it exceeded 80,000 servicemen, accompanied by more than 2,500 infantry fighting vehicles, 1,000 tanks and artillery systems, 260 multilaunch rocket systems, and 18 Iskander rocket systems. The latter can carry nuclear warheads and has a range of up to 500 kilometers. These units represent three military groupings capable of conducting rapid offensive operations against Russia’s neighbors.

Despite facing a common threat from Russia, Belarus and Ukraine operate in structurally different security environments. While Ukraine is engaged in a direct military confrontation with Russia, Belarus is Russia’s closest ally in the post-Soviet space. The network of bilateral treaties between Minsk and Moscow has led to a substantial integration of the security structures of both states. This manifests itself in the training of a considerable share of the command-level personnel of Belarus’s military and secret agencies in Russian military academies, direct cooperation between the services, and the establishment of a united military organization, which can be deployed in time

---

10 Ukrinform, “Ukraine in the OSCE: Russia has three groups of troops on the border capable of a sudden offensive,” [original in Ukrainian], July 2, 2020.
of war. These factors substantially limit flexibility in Belarus's strategic orientation of defense policy and blunt the operational vigilance of its security officials. In fact, even intelligence units that should have critical approach to threat analysis are headed by pro-Russian officials.\(^{11}\)

**The Effects of the Soviet Legacy**

The Belarusian and Ukrainian security sectors have to deal with a common palette of problems inherited from the Soviet Union. The main vulnerability is a lack of transparency and accountability that impedes objective scrutiny of the security sector, including budget planning, resource allocation, and analysis of external threats.\(^{12}\) The security sectors in Belarus and Ukraine do not have a culture of cooperation with civil society organizations, which could provide additional niche expertise in certain cases. Both countries suffer from a shortage of qualified personnel in such critical domains as strategic analysis, cyber protection, and countering propaganda. Generally, conservative security cultures are very inert and are characterized by internal resistance to reforms, especially when CSOs are trying to set the agenda by directly cooperating with security officials.

Moreover, effective democratic control though parliamentary institutions is absent in both countries. In Belarus, despite the existence of the parliamentary commission on defense, existing mechanisms are relatively superficial. This is due to unclear legal procedures, but primarily because of the politically dysfunctional nature of parliament itself—between 2010 and 2016, deputies initiated three of 417 draft laws examined by the parliament.\(^{13}\) As for Ukraine, experts usually agree that temporary investigative commissions of the parliament are politically motivated and they do not possess the necessary powers to summon state officials, which is the main reason why its reports usually do not produce tangible results.

---

11 Reformation, "Main Intelligence Directorate of Belarus headed by an adherent of the 'Russian world'" [original in Russian], July 7, 2020.

12 Interview with Ihor Kozii, military expert at the Institute for Euro-Atlantic Cooperation, September 20, 2020, Kyiv, Ukraine.

Even highly efficient security sectors may only partially mitigate the consequences of hybrid activity because subversive actions do not target state structures exclusively but are more often directed against society at large. In different contexts, an opponent mainly exploits target-specific vulnerabilities. Besides, particular economic and informational domains usually fall beyond the competence and resource capacity of security actors, and defending them inevitably requires coordination with a much larger set of state and civil institutions. That said, the most critical point for counter-hybrid efficiency is found in the ability to realize a “whole of society” approach to state security. This implies combining the efforts of actors that are streamlined against actual threats. Only such an inclusive approach will produce the necessary synergy to repel malicious hybrid acts.

Responses under authoritarianism and democratization

In this paper, resilience is taken as the capacity of a system to withstand, recover from, and adapt to negative influence. Here, the system in question is a state’s security sector, which serves as the main safeguard mechanism against hybrid threats.

Measuring the transformation of a security sector requires a variety of methods. One is to examine relevant indexes of resilience. Such quantitative measurements can be grouped according to three aspects: the quality of security provision, governance standards, and the overall level of national cohesion. The latter implies assessing the inclusiveness of the political system and its capacity to generate consensus among all stakeholders.

Data from the Stockholm International Peace Research Institute on military expenditure per capita demonstrates how much Belarus and Ukraine have invested in defense capability over the last six years. This indicator provides a state-centric and objective view of the provision of security services. Figure 2 illustrates that Belarus invested more heavily in its defense than Ukraine before 2014, and that only in 2016 did this change.

The society-oriented perception of security provision is reflected in the Societal Safety and Security composite index by the Institute for Economics and Peace. This analyzes, among other things, instability and political terror, perceived criminality, and

---

the number of the imprisoned population—all factors providing a base conducive to the destabilization of the situation via hybrid manipulation. The index uses a scale from 0 to 5, with a country more prone to peace the lower its rating is.

Figure 3 shows that Belarus has had a positive trend in recent years in addressing societal safety and security. However, the data does not take into account the 2020 unrest in the country after the presidential election, which has been accompanied by one of the heaviest crackdowns of the Lukashenko regime on civil society since 1994. Ukraine, in contrast, shows a gradual decrease in societal safety and security. Although factors stemming from the events of 2014 such as the Revolution of Dignity and the armed conflict in Donbas largely contributed to this dynamic, even before 2014 Ukraine demonstrated a performance lower than Belarus in human-oriented security.

Finally, the evaluation of security-sector governance is based on a combination of indexes in the Bertelsmann Transformation Index. This paper introduces a Governance Index, composed of indicators covering the rule of law, the stability of democratic institutions, and the state monopoly on the use of force. It also creates a National Cohesion Index that reflects the combined level of social integration, political participation, and consensus building. On a scale of 0 to 10, from negative to positive, these two indexes illustrate efficiency in governance mechanisms and cooperation among stakeholders in the security sector in particular.

As Figure 4 shows, Belarus, while being more effective than Ukraine in the provision of security, has a much weaker governance system as well as dysfunctional mechanisms of political participation and consensus-building.

Source: Bertelsmann Transformation Index
The rigidity of state institutions is the main vulnerability for the majority of authoritarian regimes. They function rather effectively as long as conditions of the basic social contract are fulfilled—moderate economic growth and security in exchange for submission to the political status quo. In case of Belarus, however, the state under condition of turbulence triggered by economic shock, civil upheaval, and hybrid interventions cannot flexibly adapt to rising challenges. In other words, the siloed security system is unable to manage hybrid activity while it is isolated from society. Hybrid actors, such as Russia, may use this gap between the state and society to further weaken national cohesion and impose their own agendas.

Ukraine: Moving Forward Unsteadily
The transformation of the security sector in Ukraine was triggered by direct military aggression by Russia. This forced officials to implement reforms while under systematic shocks induced by Kremlin's hybrid destabilization activities. They were supported by international actors and became the subject of a solid national consensus. Nevertheless, systematic constraints in the state and the continued confrontation with Russia impeded a fast and comprehensive upgrade of the security system.

By studying their country's experience with hybrid wars, Ukrainian officials have made a gigantic leap forward in reforming the security sector since 2014. Ukraine substantially reshaped the main doctrines driving the evolution of its security sector. The adoption of new doctrines in the military (2015), cyber (2016), and information security (2017) domains as well as the upgrading of the National Security Strategy in 2020 have underpinned an institutional tectonic shift and provided the necessary vision for the reform process. The 2020 strategy introduced the notion of resilience as one of its main principles, which is an essential component for the effective counteraction of hybrid activity.

The 2020 budget for national security and defense reached 5.45 percent of GDP, one of the highest levels in Europe. Although the allocated financial resources remain insufficient to cover the needs of a country engaged in an armed conflict, Ukraine's leadership managed to launch a package of urgent reforms in the security sector. The main achievements in the context of resilience to hybrid threats are:

- The rapid introduction of NATO standards, including implementation of the J-standard command structure in the General Staff and extensive training of tactical-level unit commanders.
- The adoption in 2020 of a law on defense procurement and the start of the process of corporatization in the military industrial complex, framing a system for provisioning the armed forces with the necessary materials and equipment which is more transparent and less prone to corruption;
- A conceptual reshuffle of the intelligence ecosystem through a law on intelligence in 2020 that outlined a clear separation of responsibilities between secret services and improved coordination in the intelligence community.
- The creation of the Main Situational Center under the National Security Council, representing a single point of contact for the continuous monitoring of threats and the accumulation of data from different state agencies and open-source databases.
- The substantial enhancement of information sovereignty through defining institutional responsibilities in fighting disinformation and propaganda, and increasing Ukrainian content in the national media as well as promoting the growth of civic initiatives.

Nevertheless, the focus on the strategic vision and its inconsistent operationalization put the security sector in an unsteady interim state. In some cases, this has resulted in exposure of additional vulnerabilities.

---

17 Interview with Oleg Zhdanov, military expert, Armed Forces Reserve Colonel, August 30, 2020, Kyiv, Ukraine.

18 Governmental Portal of Ukraine, “Defense Ministry’s budget for 2020 will be the largest since Ukraine’s independence”, November 19, 2020.
Specifically, many experts have pointed to the general weaknesses of the security governance apparatus that was put in a state of limbo by massive reform processes. Ukraine lacks a clearly defined model for the future of its armed forces. The first all-encompassing State Program on the Development of the Armed Forces 2017-2020 for the most part contained general provisions without the operational specifics of their implementation. Although the main text is of some use, the pace of the reform implementation remains sluggish, being constrained by bureaucracy and by generational and value gaps between officers with a Soviet worldview and those who received Western training.

Despite increased financial allocations for defense procurement, procedural inconsistencies and a fragile economy have impeded full implementation of the budget and delayed the delivery of weapons and military equipment to the armed forces. Urgently needed reform of territorial defense, initiated in its first form in 2015, still has been neither implemented nor received approval for its modalities. Along these lines, personnel turnover in the armed forces in 2018-2020 reached 77,000 people, almost a third of all contracted staff. The main reason is not insufficient social security and salary benefits—after 2014 many Ukrainians chose to join the military out of patriotism—but the preservation of Soviet-style management and governance standards. The military has a repressive command culture in which soldiers are perceived as fighting entities that do not need too many rights and mechanisms for their protection.

The transformation of one of the most important agencies in the context of hybrid resilience, the Ukrainian Security Service, had not been accomplished as of 2020. This service had the highest level of infiltration and crossing over to the Russian side in 2014. In addition, it concentrated extensive authority in its hands under umbrella of fighting economic crimes, leading to abuses of power and corruption. Officials are struggling to find a balance between shrinking the competences of the service and preserving its ability to perform assigned functions in the face of Russian aggression.

The establishment of an effective mechanism for democratic and civilian control over the security sector still faces many questions. The improvement of transparency, collaboration with civil society, and the expansion of parliamentarians’ competences to conduct investigations usually require constitutional changes. In this regard, intelligence reform, governance, and independent oversight projects have been largely overlooked by international donors, whose initiatives have concentrated mainly on the provision of other forms of technical assistance.

Moreover, implementation of the 2017 Information Security Doctrine is far from complete. The problem mainly concerns the separation of responsibilities between institutions. The Ministry of Foreign Affairs also still has not presented a viable concept of public diplomacy, illustrating the absence of a structured approach toward strategic communications that leads to the poor promotion of Ukrainian interests abroad.

Belarus: Tango of Autocracies

In the context of countering hybrid threats, Belarus’s autocratic regime possesses some advantages in comparison to transparent democratic states. A centralized management structure facilitates swift decision making and implementation. In contrast to the oligarch-influenced political environment of Ukraine where different groups compete to control financial flows, the monolithic Belarusian state appa-
ratus with its clear hierarchy is able to mobilize quicker in response to threats. Not being constrained to the same extent by the rule of law as democracies, the Lukashenko regime possesses a much wider toolkit of measures. At the same time, a political field cleared of real opponents of the regime provides a much narrower base for manipulation by external actors.

These strengths, however, negatively affect other components of national resilience. First, authoritarian systems do not have pluralistic perceptions of risks and threats, and the competition of views is determined mainly by the level of access to the autocrat. Second, the constituent parts of a centralized apparatus have a low level of autonomy. In the security sector this manifests itself in the blind implementation of orders and increased chances of system paralysis if the higher chain of command does not communicate appropriate instructions. Third, a non-democratic state is immune to disinformation only in theory. In practice, restrictions imposed on NGOs and independent media substantially limit the capacity to respond to fake news and propaganda.

Overall, the transformation of the Belarusian security sector has been limited primarily to two dimensions: updating doctrinal visions and restructuring the response capacity of the security agencies. The former led to the adoption of the new military doctrine in 2016, an information security concept in 2019, and two consecutive five-year country defense plans. Together with putting more emphasis on the risks of internal destabilization, the authorities have prioritized the development of special operations units, territorial defense, and the building up of communications, reconnaissance, artillery, and missile forces. This has resulted in an increase in hybrid, scenario-based military exercises and rather controversial attempts to reduce technological dependency on Russia in the military domain by expanding cooperation with China and boosting local production capacities.

However, the implementation of these different measures have suffered from inconsistency and a “Band-Aid” approach. Despite having upgraded doctrines, the mechanisms of threat analysis by state structures remain constrained by ideological clichés and have not adapted to the nature of hybrid activity. The absence of a fully inclusive public dialogue on security issues and a tradition of not perceiving Russia as a possible source of threat lead to major challenges to national security being neglected. In fact, these analytical structures tend to validate already adopted, politically biased decisions rather than formulate new initiatives. Coupled with Soviet-era-rooted hostility to all things Western and Russia’s legal status as an ally, the objective analysis of information is often replaced by the reproduction of Russian propaganda narratives, especially in the context of foreign policy issues. As a side effect of this analytical paralysis, the main impulses for state development are based on external events rather than coming as a result of internal discussion.

Similarly, the concept of information sovereignty remains at the level of rhetoric. While legislation provides instruments to regulate the media environment rather effectively, the available toolkit is not applied against the domination of Russian media content in the local information space. Moreover, the interpretation of the international agenda is outsourced to the Russian media while the Belarusian media focuses primarily on domestic issues.

Another weakness is the underdeveloped practices of strategic communications either domestically or toward a foreign audience. Situations when the state apparatus struggles to clearly communicate its version of events or to provide appropriate levels

24 Interview with Yuri Tsarik, deputy director and head of Russian and post-Soviet studies of the Center for Strategic and Foreign Policy Studies, April 15, 2020, Minsk, Belarus.
25 Interview with Arseny Sivitsky, director of Center for Strategic and Foreign Policy Studies, April 20, 2020, Minsk, Belarus.
26 Interview Andrei Yeliseyev, research director of the EAST Center, April 23, 2020, Warsaw, Poland.
27 Interview with state official.
28 Interview with Yeliseyev.
29 Yeliseyev and Damarad, Disinformation Resilience in Central and Eastern Europe.
of transparency on policy issues result in speculation and the hijacking of the narrative by foreign media. Recent examples include hiding details on the course of negotiations with Russia over integration under the Union State Treaty and the official position regarding the spread of coronavirus in the country.

As a result, despite formally adapting to the hybrid environment, the Belarusian security sector still lacks key components. The primary limitation is that state agencies put the protection of the regime ahead of the national interest, which was demonstrated after the 2020 presidential election. This explains why viable mechanisms of cooperation with expert NGOs and civil society overall are not developed or, at best, imitated via networks of state-sponsored civic initiatives. Without an open exchange of ideas and a structured dialogue between state and society, the development of nationwide resilience is doomed.

Another drawback of the Belarusian security system is the absence of real oversight mechanisms by the civilian sector. Parliamentary procedures are dysfunctional due to the symbolic character of the parliament, whereas options for scrutiny by NGOs and the independent media are largely restricted and associated with a high risk of state persecution.

**Better resilience against hybridity**

With all the discrepancies in different views on hybrid activity, only a whole-of-society approach to security can lead to a comprehensive response. This implies the involvement of not only security providers but also politically accountable management structures, democratic oversight institutions, and active cooperation with civil society actors in setting agendas, elaborating proposals, and control over implementation. The convergence of interests between state structures and society as well as the inclusiveness of the representation mechanism determine the level of national cohesion, which is a basic precondition for resilience against hybrid threats.

All security-sector actors should pool their capacities in three areas: awareness, coordination, and ability to respond. Awareness involves the identification of key internal vulnerabilities and monitoring the external environment for risks. Possession of the relevant information would be of little use without proper coordination among different actors inside the security system and with external partners. Cooperation does not only mean an exchange of information; it also focuses on the allocation and redistribution of resources needed in times of crisis. Finally, the response capacity encompasses mechanisms of appropriate reaction to emerging threats, including targeted countermeasures and the reduction of any power vacuum and lack of knowledge that can be exploited by hybrid actors.

In general, the internal power structures in Ukraine and Belarus restrain the scope and depth of transformations in their security sectors. For Ukraine, the clan-oligarchic economic model is the main reason for state dysfunction. Its preservation inevitably leads to increased corruption and the penetration of crime into officialdom, including in the security domain. In Belarus, the main function of the security sector is to protect the regime in exchange for a relatively stable level of social wellbeing. Generally, intertwined mechanisms of cross-sectoral control by the ideological apparatus and the secret services maintain a relatively high level of loyalty among the security personnel. The extent to which these bodies are ready to counterbalance hybrid activity from Russia depends on the level of threats posed to Lukashenko’s position specifically.

Nevertheless, measures to foster the resilience of both countries to Russian hybrid activity should target the three areas indicated.

**Improving Awareness**

On the awareness level, the Belarusian state services need first to reconsider their practices of threat analysis and move away from Cold War bipolar thinking. Even though constrained by the country’s status as a Russian ally, monitoring and analysis of Russian

---

31 Vitalii Martyniuk (ed.), *Hybrid Threats to Ukraine and Public Security*. 
activity by intelligence agencies is paramount and feasible. Taking into account the restricted character of special services’ functions, extending their focus depends primarily on political will in the governing structures. In that regard, placing regime security ahead of the national interest should no longer be the priority for the security services as it prevents them from focusing on clandestine hybrid activities targeting the population.

Together with the external dimension, stronger priority should be given to the identification of internal vulnerabilities as possible targets of hybrid actions. However, this should not be performed through internal audit by the institutions concerned only, but also by ones that do not have direct subordinate links with the agencies under inspection. Expanding the mandate of parliamentarians to conduct such comprehensive security audits is one option.

For Ukraine, awareness can be further enhanced by acting in three directions: implementing laws and doctrines, increasing transparency, and enhancing democratic oversight mechanisms as well as fighting infiltration in the security sector.

The first dimension primarily requires the finalization of the intelligence reform and institutional upgrade of the security service. The recently introduced format for the intelligence community should foster better coordination and the separation of competences among secret services. Removing from the security service its largely abused economic-overight functions and channeling its activity exclusively into counterintelligence are the primary objectives of the transformation that is under way. In addition, effective protection against disinformation necessitates the adoption of tactical-level documents to detail information-security doctrine. This is required to define the responsibilities of all stakeholders that are currently described only at a high level.

Second, procedures for democratic oversight of the security sector remain dysfunctional. Additional steps with regard to legal and corporate culture are needed to equip the parliament with viable instruments of oversight. Increasing transparency and reforming the overly restrictive notion of secrecy in the security sector could produce a powerful impulse for civil society to actively engage in oversight activities. For example, the introduction of electronic systems for procurement, human-resource management, logistics, and property management could substantially decrease corruption in the sector.32

Lastly, the problem of infiltration in the security structures is generally ignored at the state level. Ukraine’s authorities are still struggling to develop an approach to deal with this problem, which led to considerable losses during the aggression by Russia in 2014. Bearing in mind the absence of a statewide policy on the matter due to its sensitivity, agencies should enhance their internal protocols to screen officials and new applicants against possible affiliation with foreign secret services.

**Working Together**

In the sphere of coordination, the main drawback of Belarus’s overly centralized security sector comes

---

from its main strength. Whereas there is swift decision making across the system, the ability of its constituent parts to act autonomously is very limited. The rigidity of the sector leads to a situation in which personnel are generally afraid of taking the initiative and limit their contribution to the implementation of measures approved at a higher level.

In the context of countering hybrid activity, a centralized and repressive corporate culture usually impedes interagency communication and sustains siloed activities. In fact, personnel tend to rely on approval from the higher command rather than perform duties in accordance with their assigned mandate. Unfortunately, overcoming this paralysis is possible only by changing the incentives inside the system. In the current situation, appreciation within the bureaucratic system is earned through blind loyalty rather than meeting transparent performance indicators, which is important for the security of the state. The presence of an objective judicial system that is able to protect the rights of public officials is also very important.

Moreover, the Belarusian security system lacks an integrated analytical component. The proper analysis of hybrid threats requires the establishment of a common situational center capable of drawing insights from a variety of sources and formulating actionable countermeasures. For that reason, the capacities of the State Security Council should be revisited to enhance its analytical competency. This cannot be done without restructuring the intelligence services and correcting their analytical culture.

In addition, establishing structured mechanisms of cooperation with civil society may resolve issues pertaining to the lack of qualified staff and expertise in the state security sector. Recent examples of such cooperation were primarily limited to the Ministries of Foreign Affairs and Economy. New areas of cooperation might include strategic analysis, cybersecurity, fighting disinformation, and performing sociological studies. It is essential not to impose such cooperation from the top, but to foster a bottom-up approach and stimulate civic initiatives able to abide by the rules of the state bureaucracy.33

More coordination also needs to be developed among NGOs and expert initiatives, including at the regional level. The work of research institutions and think tanks working on Belarus remains largely scattered. The problem could be resolved through developing non-government-affiliated platforms that could provide an inclusive venue for the exchange of opinions.

In the context of countering hybrid activity, a centralized and repressive corporate culture usually impedes interagency communication and sustains siloed activities.

From a coordination perspective for Ukraine, the National Security and Defense Council should start playing a more active role in aligning policies across sectors and should not limit itself to principally being a coordinating body. Whereas the substantial recalibration of its competences would require constitutional changes, effective operational engagement can be achieved within the scope of its current competences. In this way, the creation of an intelligence “community,” as proclaimed by the new Law on Intelligence, should be further formalized to support not only interagency communication among the secret services, but also interaction with other national security actors and foreign partners.34

Crucially, attention must be paid to the state of the morale of the personnel in the armed forces. The gradual transition from a Soviet command culture to having more decision-making responsibilities at the tactical-unit level necessitates functioning mechanisms to protect the rights of members of the military. This is especially crucial for non-commissioned

33 Interview with Tsarik.
34 Interview with Zhdanov.
officers, who play a more important role in the operational activity of units in NATO's command culture. The authorities could consider establishing a military ombudsman. This office would be independent from the Ministry of Defense and possess competences beyond a consultative role. Moreover, the ombudsman's representatives should be accessible not only in the capital but also in units' actual locations.

Ukraine's anti-corruption system should concentrate more on large criminal cases rather than on the prosecution of certain officials for incorrect income and assets declarations. Even though growing transparency and accountability is positive, intolerable cases of public theft through oligarch-controlled schemes have not received proper attention from state investigators and prosecutors. Moreover, problems in delimiting competences, internal conflicts, and poor coordination inside the rapidly expanded system of anti-corruption institutions are still prominent. Overlapping functions and untimely legislation provoke situations in which the same case may fall under the jurisdiction of several agencies, including the security service and police.

**Providing Resources**

In the sphere of response capacity, Belarus and Ukraine experience large problems with strategic communications.

Despite the fact that the Ukrainian government has made rapid progress in communicating its policies to the population and foreign audiences, it still lacks resources and mechanisms to promote a national narrative abroad, including fighting Russian propaganda by its own means. In this regard, Ukraine remains very dependent on its Western partners. This gap should be filled by, among others, a more active public diplomacy coordinated via the Ministry of Foreign Affairs, and the organization of educational programs in fact-checking and open-source intelligence for media specialists.

As for Belarus, the government frequently neglects to communicate state policy transparently and reacts quite unprofessionally to criticism from civil society or pro-Russian media outlets. This approach decreases trust in public institutions and leads to the uncontrolled dissemination of propaganda false narratives among the population. The authorities should transition from their rare reactive communication campaigns to the comprehensive, proactive protection of Belarusian culture, language, and statehood from attacks.

Belarus and Ukraine experience large problems with strategic communications.

When it comes to internal communications, public officials should align their decisions with proper studies of public sentiments and reconsider the Soviet-rooted culture of suppressing criticism and avoiding dialogue. The latter may help to avert or at least decrease the level of uncontrolled social discontent leading to internal political destabilization.

Second, the Ukrainian and Belarusian economies are not able to sustain fully professional armed forces. Officials therefore should establish effective territorial defense systems. This might combine elements of the Swiss, Finnish, or Estonian security sectors. Both countries need to step away from the clearly repressive post-Soviet method of involuntary service and introduce more flexible formats. The total period of general service should cover only combat-related activities and should provide essential training. As in the Swiss model, a basic course could be accomplished over several years without drastically isolating recruits from the labor market.

Territorial defense might follow as the next stage of the service while being voluntary and community-based. Recruiting centers should incentivize recruits to receive additional training by offering courses in

---

35 Interview with Kozii.

36 Interview with Samus.
skills relevant to the private sector as well. The state also needs to introduce additional social guarantees to make military service more appealing. Such measures could include special benefits for enrollment in higher education institutions or for competing for public state positions.

Coordinating cooperation with civil society might lead to better contributions to state defense. Civil initiatives need to be channeled via specially dedicated civil-military officials in recruitment centers. Such representatives could act not only as liaison officers, but also as coordinators in crisis situations, including through their engagement with volunteers.

**Moving Forward**

These transformations first require an evolution of mentality among high-ranking security officials, rather than simply extending financial allocations. They involve for the most part overcoming communications and value gaps between the state and civil society sectors, as manifested in Ukraine after a wave of new civic initiatives. A substantial number of personnel with open minds should first be placed in state security institutions before the authorities can move away from Soviet-based practices of security management and recruitment. This might be fostered in part by extending exchange and training programs with Western partners.

Additionally, some of the identified gaps require the active involvement of international organizations and institutions.

In the case of Belarus, there is a clear phenomenon of “Westlessness,” mainly manifested in an insufficient level of support for civil society and a rather mild reaction to the repressions by the regime. Possible initiatives in that direction include:

- Adoption of a coordinated position toward Belarus, including by putting more pressure on the authorities concerning human rights violations and extending support to civil society. Besides, learning lessons from the Ukrainian case, the EU and the United States should not neglect Russian interests in the matter and should not exclude Russia from negotiations as the actor having the most serious leverage on Lukashenko.

- The development of large-scale assistance package for the recovery of the economy in exchange for the democratization of the state system, judicial reform, and the restoration of the rule of law. Separate funding is required to protect and support victims of repressions.

- Increase of investments in information technology companies and startups targeting domain of civic technology. It includes initiatives increasing transparency in the provision of state services, the self-organization of people, and the preservation of national heritage. The extraterritorial nature and relative anonymity of IT sector allows it to operate from abroad without major disruptions in providing relevant services. Recent examples include online platform Golos that designed a secure and reliable way for counting votes and operated on a voluntary basis without any external assistance.

- The extension of support programs for Belarusian culture and language aimed at the further enhancement of national identity and the cultivation in the local population of a sense of ownership of the future of the nation.

- The provision of better coordination, funding, and platforms of exchange of opinions among students, experts, and civil society organizations, including at the regional level. Preference might be given to sharing expertise with Western research institutions specializing in hybrid threats, media literacy programs, and support for independent media.

In the case of Ukraine, international donors should move from predominantly grant-driven programs to be more receptive to bottom-up demand from civil society in relation to the required projects. This envis-

---

ages the active involvement of local CSOs in assessing the development aid and in project mapping. Other steps might include:

- Stricter and clearer prospects-driven positioning in the implementation of agreed priorities, specifically in anti-corruption and security-service reforms. This could include outlining a clear roadmap for Ukraine in terms of future accession to NATO, including by issuing a Membership Action Plan.\(^{38}\)
- Avoiding tunnel vision, in which conditionality is stressed in relation to anti-corruption projects whereas reform of the security sector does not attract such attention. Even though the protection of investments in the country might seem to be the most important goal to international partners, achieving a secure and attractive business climate is closely linked to defense sustainability, accountability of the secret services and law-enforcement agencies.
- Greater support to democratic oversight initiatives in the security sector and particularly reform of the intelligence system. The European Union Advisory Mission should be more vocal in pushing for reform of the security service, which is part of its mandate in the country.
- Introducing a single, publicly available online platform to track development projects with standardized classifications and descriptions. This would help to trace existing projects, identify underfinanced areas, and avoid duplication. The same source can be used for the submission of proposals and could serve as a crowdfunding platform.

Prospects for Achieving Anti-Hybrid Resilience

The transformation of the security sectors in Belarus and Ukraine represents contrasting examples of reactions to the changing geopolitical environment in Eastern Europe and the increasing threat from Russia. While having identical problems and similar security risks, the specifics of their political regimes as well as local constraints have determined the different responses of both states to hybrid threats.

Unfortunately, the 2020 violent crackdown on civil society and the serious rule-of-law crisis in Belarus have inevitably engendered long-standing negative repercussions for the country. The sharp decrease in trust in public institutions, and in the security sector in particular, has widened the divide between the state and civil society, and has launched a polarization process within the Belarusian nation that could only be reversed after many years of transformation. The primary consequence of this is the extreme weakening of national cohesion, which is the basic precondition to effectively rebuff hybrid activity. In fact, the current political situation in Belarus provides one of the most conducive environments for hybrid intervention and for manipulation of social consciousness.

\(^{38}\) Interview with Kateryna Zarembo, associate fellow at the New Europe Center, October 15, 2020, Kyiv, Ukraine.
latter leads to shrinking numbers of reform proponents, society polarization and negatively affects prospects of the long-standing strategic engagement between the state, civil society, and international partners.

The main challenge now consists in implementing mechanisms to gradually, and yet visibly, eradicate corruption, increase accountability of security providers and leverage civil society expertise and potential in oversight over security sector. It is essential to understand that these steps are critical for creating structural preconditions for the transformation of the oligarch-based economic model.

All in all, the securitization of the regime in Belarus and the systemic corruption leading to state dysfunction in Ukraine are the primary factors hampering the transformations required to enhance their resilience against hybrid threats. Remaining gaps inside their respective security sector can be filled only with synchronized engagement at the national and international levels. At the same time, the capacity of all involved actors to remove revealed limitations will largely determine the prospects of both countries to resist hybrid attacks from Russia, and hopefully, formulate a coordinated regional response.
This work represents solely the opinion of the author and any opinion expressed herein should not be taken to represent an official position of the institution to which the author is affiliated.

About the Author(s)
Pavel Hanchuk is a Rethink.CEE fellow at the German Marshall Fund of the United States. Originally coming from the defence sector, his areas of expertise include international security cooperation, arms control, threat analysis, and risk assessment. He completed professional training programs in information analysis (Belgrade, Serbia) and crisis management (NATO School Oberammergau, Germany). He holds an MA in EU international relations and diplomacy studies from the College of Europe (Bruges, Belgium).

About the ReThink.CEE Fellowship
As Central and Eastern Europe faces mounting challenges to its democracy, security, and prosperity, fresh intellectual and practical impulses are urgently needed in the region and in the West broadly. For this reason, GMF established the ReThink.CEE Fellowship that supports next-generation policy analysts and civic activists from this critical part of Europe. Through conducting and presenting an original piece of policy research, fellows contribute to better understanding of regional dynamics and to effective policy responses by the transatlantic community.

About GMF
The German Marshall Fund of the United States (GMF) is a non-partisan policy organization committed to the idea that the United States and Europe are stronger together. GMF champions the principles of democracy, human rights, and international cooperation, which have served as the bedrock of peace and prosperity since the end of World War II, but are under increasing strain. GMF works on issues critical to transatlantic interests in the 21st century, including the future of democracy, security and defense, geopolitics and the rise of China, and technology and innovation. By drawing on and fostering a community of people with diverse life experiences and political perspectives, GMF pursues its mission by driving the policy debate through cutting-edge analysis and convening, fortifying civil society, and cultivating the next generation of leaders on both sides of the Atlantic. Founded in 1972 through a gift from Germany as a tribute to the Marshall Plan, GMF is headquartered in Washington, DC, with offices in Berlin, Brussels, Ankara, Belgrade, Bucharest, Paris, and Warsaw.