# NATO RESILIENCE STRATEGY TOWARDS RUSSIAN HYBRID WARFARE

**Liliana FILIP**

**National University of Political Science and Public Administration, Bucharest, Romania**

*Faced with the greatest security challenges of this generation, the Nord Atlantic Alliance is currently implementing the most significant strategy for strengthening its collective defense capabilities since the end of the Cold War. While the public attention has focused on NATO's military adaptation, the concerted efforts to strengthen the Alliance's ability to withstand and recover from a military attack, have so far been less visible. However, this is changing. At the 2016 Alliance high level meeting in Warsaw, NATO leaders agreed on an unprecedented commitment to "increase resilience". The 28 Allies work urgently to put this commitment into practice. But how to understand this NATO resilience?*

**Key words:** *resilience, hybrid warfare, cyber space, emerging threats, civil preparedness, civil-military readiness.*

## 1. INTRODUCTION

Already during the Cold War, resilience has been conceptualized to anticipate and resolve disruptive challenges to critical functions and to improve combat as direct or indirect attack. However, given the intensification of globalization, the evolution of technology and the vast and precise information, the diversity of communication channels as well as the evolution of resistance to hybrid warfare, the concept needs to be reinvented for the information and knowledge era, starting from the premise that there is a strong interconnectivity between civil, private and military sectors. (Joseph S. Mayunga, 2007)

The renewal of the Alliance's focus on resilience is based on the recognition of two inconvenient but increasingly important trends. First of all, today's armed forces are increasingly dependent on the capabilities and infrastructure that are owned or operated by the civilian environment. To ensure access to these capabilities, NATO requires a solid civilian training in the allied nations, both in the public and private sectors.

Secondly, civilian services and infrastructure are potentially vulnerable to external attacks or domestic problems - and such vulnerabilities could be exploited by potential opponents. Not only could the Alliance's military capabilities be indirectly attacked, but civilian functions could become a major target. In a time of hybrid threats, strengthening resilience, primarily by improving civilian training and cyber defense, is therefore a critical component of NATO's efforts to discourage and defend against the whole range of threats.

## 2. DEFINING RESILIENCE IN SECURITY

The term "resilience" is used in many contexts. The concept has been appealing for areas that involve the management of complex interconnected systems, and has therefore spread beyond its initial use in ecology. It is now applied at different levels (individual, community, state) and in various fields such as psychology, infrastructure management, economy, organizational management, community studies, etc.

Until now, the most popular use in the field of security has been in the human disaster preparedness and counter-terrorism. In the area of cyber security and critical infrastructure protection, it can be considered that they are still working.

Following Russia's promotion and implementation of hybrid warfare, resilience is now a popular concept within NATO and the EU, conceived as a way to build a strategic and holistic response to this threat, combining perspectives such as "the whole government", "the whole society" and "the whole alliance", thus applied in multiple areas of interest for the security zone.

In general terms, resilience has been defined as "a process linking a set of adaptive capabilities to a positive path of operation and adaptation after a perturbance."

This definition implies that resilience is a process, although it can also be seen as a strategy or as "the ability of a system to maintain its functions and structure in the face of internal and external changes." (Brad Allenby and Jonathan Fink, 2005)

It is based on certain system resources and the dynamic attributes of those resources (robustness, redundancy, speed). This perspective allows for a proactive approach to build resilience by accumulating the necessary resources in a system and ensuring that these resources possess the necessary dynamic attributes at a time when disturbances occur.

System managers can thus develop policies (such as principles, norms and standards, investment priorities) that lead to resilience. This is especially true for enhancing cyber security.

The EU's global strategy defines resilience: "the capacity of states and societies to reform so they resist and recover from internal and external crises," which aligns well with the generic definitions of resilience described above. This reflects that the EU's understanding of resilience refers to change, adaptation and recovery capacities. The emphasis on reforms stems from one of the key of the EU - the projection of its soft, normative, stabilizing, reforming and transforming power of countries requiring membership or associate status. However, when it comes to internal resilience, it is more about critical infrastructures, networks and services than about values, norms, institutions, or reforms, rather than something that has to be protected against the attempts and erodes Member States from within.

NATO focuses on infrastructure, civilian training, continuity of services, accumulation of reserves and access to them, as well as various procedures that facilitate a rapid response to the crisis. Its major concern is that the Alliance relies heavily on the private sector when it moves, deploys and supports its forces; therefore, pays great attention to civilian capabilities and civil-military interaction.

This is understandable given its role as a "military response" and "multiplier of force" in military conflicts. Like the EU, it should not neglect its role of helping countries - both allies and partners - to maintain their capacity to reform themselves in the face of adversity.

As Jamie Shea also noted (Jamie Shea, 2006), NATO and EU roles in supporting the resilience of the most vulnerable and exposed countries often overlap, especially in areas such as cyber security, strategic communication, civilian preparation, and combating Russia's hybrid war.

Although Russian hybrid combat techniques have been extensively analyzed, it is difficult to predict when, where and what types of interventions will be created and exploited by Moscow or other adversaries - to attack / affect the target countries. Russia's approach usually combines both the application of long-term pressure (e.g. hostile propaganda and economic warfare) and the opportunistic administration of sudden shocks in the short term, making it impossible to identify a single set of capacities needed to counteract hybrid strategy.

Enhanced resilience of potential targets - allies and partners - addressing a wide range of vulnerabilities is of vital importance if NATO, in cooperation with the EU, tries to block Moscow from reaching its political and strategic goals in relation to the Alliance and its partners.

Equally important is the alliance's correct assessment that Russia will continue to undermine NATO's legitimacy and credibility so that nations feel helpless and have no choice but to accept Moscow's geopolitical demands. The alliance's efforts - through strategic communication, public diplomacy and public mobilization - to ensure a high level of trust and support in its core tasks, policies and strategies among the general public of allies and partners, and the constant belief that "no one will not be left behind" when encountering difficulties, are fundamental to counteract this. It is just as important that NATO's proactive efforts remain legitimate, relevant, visible, coherent and credible in terms of supporting the most vulnerable nations (so-called "forward resilience").

In strategic terms, resilience can be seen as a deterrent or "the conviction of the enemy not to attack by believing that his attack will be defeated - that means that he will not be able to achieve his operational goals." (David Yost, 2003)

Hybrid war strategy - is essentially a strategy designed to cause disturbances, confusion, destabilization, and paralysis (for example, modeling the behavior of the target nation) - and can be countered by demonstrating that all of these goals are not achieved due to the strength of the target.

E.g.:

- a high level of the competence of a society in critical thinking and the understanding of the nature of such hybrid war instruments, such as hostile propaganda, political extremism, social protest campaigns or military intimidation - along with the trust of society in the integrity of the political system, the leadership policy and government communication - can eliminate the benefits of these instruments.
- a strong sense of belonging to a community, citizen empowerment and economic equity, as well as mutual support available, reduce the potential for division and polarization of society and the countering of various groups of society against the others and against the nation's institutions.
- a high level of volunteering and civic participation in state actions, when promoted by national security and defense institutions, substantially strengthens these organizations in front of their adversaries.
- measures aimed at seriously disrupting economic activities (e.g. sanctions, energy supply disruptions, financial destabilization, etc.) fail to achieve the desired long-term effect when faced with high levels of economic development.
- theabilityofcriticalinfrastructure, including communication and information systems, to absorb the impact of sabotage or attacks, rapid adaptation and continued delivery of a satisfactory level of service make it unnecessary to exert pressure in this way.
- sufficient and quickly accessible financial capital, basic

needs (such as food, fuel, medical supplies) and technical resources (e.g. spare parts and materials for infrastructure maintenance and repair) ensure that sudden shocks caused by aggressors does not translate into a negative impact on the nation's will to persevere.

The challenge is to convincingly prove that the vulnerabilities are really missing and that a particular society is indeed resilient from all points of view. This starts with knowing your own vulnerabilities as society and then striving to eliminate them. The problem here is that the process of addressing the different vulnerabilities can affect the power relations in nations, and therefore we must always address the pertinent question of who are the winners and losers of the process of building social resilience.

Some of these "losers" are forced to become, consciously or not, the natural allies of an aggressor in a hybrid conflict - which is evident not only in countries like Ukraine or Georgia, but even among the political or economic elites of some NATO Allies.

Last but not least, discouragement subsides into the aggressor's perception, which means that an opponent must be convinced enough that the target society is too resilient to give up the hybrid approach to war.

This is difficult to achieve, since each adversary is driven by logic's rationality and own calculations, and can assess the resilience of the target very differently. This, in turn, means that Russia will never cease to try to identify vulnerabilities and then constantly test a target nation.

Therefore, the Alliance must continually develop and maintain a profound and sophisticated understanding of its allies and partners about the vulnerabilities, resources, capabilities and potential "defeated" resilience policies, as well as about Moscow's thinking and calculations of these vulnerabilities.

The Alliance firmly assumes that cyber-domain is one of the areas in which NATO can exercise its collective power to address the critical vulnerabilities of its allies and partners and to strengthen its resilience. Perhaps this is one of the most promising sectors in which civil-military synergies, public-private partnerships, EU-NATO cooperation and the involvement of NATO partners can be pursued to achieve the desired effect. It is also the sector where negative impacts (e.g. paralyzing cyber-attacks) have an impact on several sectors of the nations (financial systems, industrial production and distribution, energy supply, foreign trade, government services, communications, media etc.).

## 3. REINVENTING THE CONCEPT OF RESILIENCE FOR NATO EFFECTIVE DEFENSE

Resilience is not a new task for the Alliance. The article III of the Washington Treaty states that allies have an obligation to develop and maintain the ability to withstand the armed attack. As has been said, “defense begins at home”.

Long before the emergence of cyber threats and hybrid war, this notion of resilience has always been understood to overcome the limits on military capabilities.

Since the 1950s, NATO has implemented policies and civilian training plans. By the end of the 1980s, the Alliance had maintained plans for eight NATO civilian agencies, which could rise in times of crisis or war to co-ordinate and direct efforts, from the allocation of industrial resources and oil supplies, food production, civil transportation, refugee flows management.

The NATO Heads of State and Government reiterated and confirmed this approach at their Warsaw Summit on 8-9 July 2016, with the commitment “to increase the resilience, it requires that all the Alliance’s members to maintain and further develop their individual capacity and collective efforts to withstand any form of armed attack. In this context, we are today committed to continuing to improve our resilience to the full range of threats, including hybrid threats, from any direction for a credible defense and effective fulfillment of the Alliance’s main tasks.” (NATO Summit Guide)

Consequently, the European Union and NATO are investing in strengthening the capacities of partner nations to fight against hybrid threats. The European Union’s global strategy provides for this purpose: “It is in the interests of our citizens to invest in the resilience of states and societies to the east stretching into Central Asia, and south down to Central Africa. A resilient society featuring democracy, trust in institutions, and sustainable development lies at the heart of a resilient state.” (Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union’s Foreign And Security Policy)

A particular importance is cooperation with the private sector. (HARRES, 2016) The army is becoming more and more dependent on infrastructure and private sector assets. NATO, for example, faces two distinct but interdependent challenges: first, ensuring that it can quickly move all the forces and equipment necessary for mission areas when faced with an imminent threat or attack; and, secondly, Member States should be able to anticipate, identify, mitigate and recover from hybrid attacks with minimal impact.

Resilient systems and organizations must maintain a certain functionality and be able to maintain control while they are being attacked. To this end, three elements are considered important:

1.the capacity to work under heavy conditions;

2.the ability to recover quickly;

3.the ability to learn from experienced attacks.

The NATO allied Command Transformation (ACT) identified four "areas of concern" with potential to increase resilience:

◆ Identifying key vulnerabilities and associated risks this allows governments to develop responses and appropriate mechanisms to manage the consequences of orchestrating all appropriate power tools both nationally and internationally.

◆ Synchronizing the trans-governmental decision-making process - combating hybrid threats requires a different government approach that covers security mechanisms better than in the past. Political and military decision-makers need to be able to handle opponents attacking their own centers of gravity.

◆ Creating military sustainability and civilian training - the civilian population is not just a potential victim; at the same time, it is a critical source of resilience. Civil education allows military sustainability, while military capabilities protect its population and prosperity.

◆ Balancing the allocation of available resources - strengthening the links between civil, private and military sectors will allow cost sharing at the same time. It provides for the development of mitigation tools, such as diversification of supply, resources and services.

Each area of interest provides a prism for discreet analysis. As a military project, resilience must be measured in terms of training, with well-defined training standards. The resilience of the civil education project must be organized with defined standards and a high level of training to achieve this. Simulation exercises based on scenarios can be a catalyst for learning in complex emergencies - for civilian and military actors, but especially for civil-military cooperation.

From the ACT perspective, these "areas of interest" could serve as a bridge between the present and the future and will provide a measurable change, given the basic question: how quickly a system attacked by any combination of disruptive effects can reach a stable status?

## CONCLUSIONS – RESILIENCE IS ABOUT NATIONAL TO INTERNATIONAL

The starting point for dealing with hybrid challenges and building the necessary resilience is the situation awareness. This requires, first of all, a common understanding of their own vulnerabilities, in other words a common assessment of the risks to their own critical vulnerabilities, their own weight centers, but also an understanding of what perceived by the opponents, as they could exploit these perceptions. We should probably take a deeper look to all this.

Dedicated mechanisms are needed for the exchange of information. The rapid identification of a hybrid attack is a critical prerequisite for timely decision making for early engagement and escalation blocking. Hybrid threat indicators and existing risk assessment mechanisms should provide for early warning.

Security risk assessment methodologies should inform decision-makers and promote risk-based policy formulation in areas ranging from aviation security to terrorist financing and money laundering. Intelligence and information exchange have become even more important. The knowledge network is essential for organizational learning and adaptation, for training and education, and last but not least for operations - thus providing knowledge that can be applied.

Exercises and training programs must reflect recent developments and responses to hybrid warfare. They will help develop a common understanding of threats and vulnerabilities, tools and mechanisms and improve integrated decision-making. (Norris and all, 2008)

To this end, common civil-military education, training and exercises - to include high-level training - must use the best possible applications in future and advanced generation learning methods - collective training and the promotion of knowledge development for interdepartmental and coalitions interoperability.

Recently, NATO ambassadors and defense ministers have organized simulation exercises and scenarios to test their awareness of the situation and their reaction to hybrid threats. Obviously, it was a wake-up call for many. Also civilian leadership and civil-private-military interaction must improve how to respond to challenging hybrid threats.

## REFERENCES

[1] Joseph S. Mayunga, “Understanding and applying the concept of community disaster resilience: A capital-based approach”, Summer Academy for Social Vulnerability and Resilience Building, Munich, Germany, 2007.

[2] Brad Allenby and Jonathan Fink, “Toward inherently secure and resilient societies,” Science, Vol. 309, No. 5737, 2005, p.1034.

[3] European Union, Shared Vision, Common Action: A Stronger Europe, A Global Strategy for the European Union’s Foreign And Security Policy, June 2016,p. 23.

[4] Jamie Shea, “Resilience: a core element of collective defence,” NATO Review, 2016.

[5] David Yost, “Debating security strategies”, NATO Review,2003.

[6] ***, NATO Summit Guide. Warsaw, 8-9 July, 2016.

[7] Edward J. Harres, „Towards a Fourth Offset Strategy,” Small Wars Journal, 2016.

[8]Fran H. Norris, Susan P. Stevens, Betty Pfefferbaum, Karen F. Wyche and Rose L. Pfefferbaum, “Community resilience as a metaphor, theory, set of capacities, and strategy for disaster readiness”, American Journal of Community Psychology, no. 41, 2008, p. 130.