POOLING THE EXPERTISE TO DEVELOP AN EARLY WARNING SYSTEM TO COUNTER HYBRID THREATS

A policy paper by

Eastern Europe Studies Centre, Lithuania

Co-organized by

Pooling the Expertise to Develop an Early Warning System to Counter Hybrid Threats

A policy paper by Eastern Europe Studies Centre, Lithuania

This activity is supported by: The NATO Science for Peace and Security Programme

About the event: Russia's intervention in Ukraine, accompanied by an unprecedented level of disinformation, challenged the post-Cold War security environment of cooperation and partnership. At the same time, Russia's activity towards NATO member states and its allies started to encompass many hybrid (non-linear, 4th generation, etc.) elements, which are clearly posing a new kind of threats to the Allies.

The achievements of Russia's non-linear campaign in Ukraine have bolstered the validity of the hybrid method of warfare. It is no coincidence that hybrid warfare has become one of the most discussed concepts among the researchers, scholars; it was also 'securitized' by politicians and military personnel. Both hybrid threats and counter-actions are being debated. However, challenges remain; for instance, in order to develop counter-measures, it is essential to answer the question of how to identify hybrid threat signals. It is ought to be done as early as possible, in order to be able to react and neutralize the threat effectively.

The experts gathered to discuss and identify the modern early warning signals of hybrid threats and the best possible responses that could be applied in each individual case of malign activity. During an intense two day conference-workshop duration experts manages to provide a wide range of recommendations on topics starting from the general history and concept of the hybrid warfare and why it is a threat, while later developing and including case studies of countries where this concept is used in practice, and finishing with experiences how and what means could be used to increase resilience to ongoing challenges.

The event took place on April 24th – 26th, 2019 in Vilnius, Lithuania.

About the Eastern Europe Studies Centre: The Eastern Europe Studies Centre (EESC) is a non-governmental, non-profit organization aiming to build civil society and promote democracy in Eastern Europe by monitoring and researching political, economic, and social developments in the region, and by developing qualitative analyses of them. EESC organizes conferences, seminars, and round-table discussions regarding issues relevant to civil society and democracy; it trains people in areas relevant to its mission; and it also offers consultations and recommendations to individuals and organizations cooperating with Belarus, Ukraine, Moldova, and Georgia. EESC specializes in the EU Eastern neighbourhood policy.

Hybrid Warfare Concept: New Techniques, Tactical Variety

When talking about the concept of hybrid warfare and the meaning of this phenomenon in general, we have to emphasize that this not a new concept at all, it is rather a new impression after a calm period. Throughout history aggressors used various means to develop instability in opposing countries and societies, such as spreading disinformation to create deeper cleavages among different groups of the society, spreading religious or ideological influence, using law fare as a weapon to justify conflicts, using energetic resources to weaken opponent's will to resist or using modern cyber and information interference to disrupt basic functioning of institutions or the society in general. When it comes to hybrid issue problematic, it has such a diverse array of instruments such as border security, migration, energy security, cyber security, disinformation and etc. NATO is predominantly at its core competence is a military power, it's a military Alliance, but it has to adapt to new security challenges that affect wider competence than hard power security.

Nevertheless, each of these fields and methods requires a separate approach in each case individually, where different tactics are being used depending on existing weaknesses that is the key element in this warfare. In other words, the resilience in these key spots against the aforementioned warfare means has to be developed in order to not lose this war.

Before going further into details, it is important to clarify what societal and governmental resilience really is, because it is crucial to always have clearly identified goals in order to achieve them. According to the expert community, the resilience is the ability of the individual; or the community; or the state, in general, to come back to the normal functioning as soon as possible after any stress caused by inner of outer actors. Hence, it is also important to make a distinction and educate society what are these threats and why citizens should see one or other activities of foreign actors as a threat to their personal security and country's national security. If national governments directly warn residents about certain selective threats and try to combat them using the same methods as an aggressor does, then they risk looking paranoid and in this way creating an unnecessary panic in the public, because the public might do not see those threats in the first place. This could be a vital mistake because it is a primary goal an aggressor, who wants to not only to deepen the aforementioned cleavages but also to break the basic principles of the political and institutional framework,

even while using already existing institutional or democratic foundation of the state. For instance, this could be legal authority and rule of law, democratic principles of the government, freedom of speech and media independence and etc.

However, there is also another approach defined by experts, that tells us that we should think not only about how to identify the threat, that constantly evolves and in each case might be different, but to put more emphasis our response to it more than on threats, because otherwise we will get stuck into the definitions and it's sometimes extremely hard even to define them. In terms of developing a warning system as a response, it involves much more than the government and armed forces. In spite of the fact NATO Alliance has huge capabilities in this field, focusing only on so-called hard power would put the Alliance in the system when it has to constantly follow actions of Russia or other actors and NATO naturally puts itself into situation where it has act reactive and not proactive while not focusing its primary targets of defense – the societies and its resilience.

The Understanding of Hybrid Threats in Practice: The West, Russia and its Neighbors

As it was described in the previous section, hybrid tools are constantly evolving so NATO naturally puts itself into a situation where it has act reactive and not proactive. It is almost impossible to fight against the unknown – we still do not know what are we facing, what do we stand against? We can clearly state that we still do not know how to manage Russian channels of a disinformation campaign, we do not know how many messengers exist that are vaping spread, we do not know how many people they persuade – it is like going into a war without knowing how many and what are our targets.

This why it is necessary to firstly adopt reactive solutions to this problem: **first** and foremost, it is necessary to document the threat on the institutional level to ensure more efficient and coordinated reaction in the government, while also getting better common understanding of what is happening; **Secondly,** gradual awareness raising both on the domestic and international level. This important due to the earlier mentioned societal reaction to the threat

and to ensure international recognition. As hybrid measures are also trying to create cleavages among different allied countries, so joined recognition and response could be much more effective than fragmented individualized issue statements by numerous countries. **Third,** repairing the weaknesses – hybrid attacks usually do not create problems as such, they are usually just exploding already existing problems by "looking for your weaknesses". While it is difficult just to avoid the natural weakness, it is strongly advised not to artificially hide any existing problem and, for instance, to use domestic disinformation and in this way to create a so-called information bubble. This action would discredit local fundamental values and institutional framework. **Fourth,** researching and indicating the most sensitive parts in the society could help to earlier develop a framework and to stop the act of aggression. This could be done on any level, for instance, constantly using opinion polls that would use resonance questions and measure the success of the disinformation campaign. We need to have more pressure on social media because they are definitely a key member of spreading this information and this is what needs to be repaired.

In the international level of the main players in the European security system is NATO. The Alliance is doing well in creating a system on gathering the knowledge how to react to any kind of hybrid threats from creating capabilities to reacting to the cyber-attacks to skills how to react to the possible armed aggression as it happened in Eastern Ukraine. But it is important to emphasize that the government bears the responsibility for resisting to hybrid threats since it is mostly responsible for relations between the government and society. However, there are still left a dilemma on the side of Alliance – should the Alliance use the response (as it is described in Article 5) and how that response should look like in the case of hybrid aggression? Cyber-attack with catastrophic consequences to the ally or allies would/could be a reason for activating article five, but beyond that, Alliance is still sort of very gray zone and discussing how it should be done. Leaving this area for interpretation could be seen as a weakness that at the same time creates some uncertainty and mistrust within members of the Alliance. This flaw must be solved on an institutional level by creating clear boundaries, otherwise, the aggressor may fragment the members of the Alliance on a case-by-case basis. Generally, we can see that argument as an adapted version of informing the society, but it is raised on the international level of Alliance.

It is important to further analyse case studies, especially cases of eastern partnership countries, where modern hybrid tactics are being actively applied. One of the countries that

have to deal with Russian hybrid warfare campaigns and its influence on the political process in Moldova. Sensitive areas of vulnerability in Moldova at the same time represent the main working channels and tools that could be used by the aggressor in other countries:

1. There is low quality of the internal political environment due to the fact that there is little or no attention paid to the political or public debate on hybrid threats. Additionally, pro-Russian political parties, such as the Socialist Party (PSRM) and Our Party (PN) openly promote Russia and convey anti-European and anti-American messages. Their main focus is promoting the narrative that Moldova is lost without Russia — that it will not survive without the Russian market, Russian gas or Russia's protection. They pretend to represent not just Russian-speaking Moldovans, but other minorities as well.
2. A constant threat of hard power and military presence in the area of Transnistria creates in the country a sense of insecurity what divides society on security priorities.
3. Unsustainable sources of economic development. Moldova is highly dependent on trade, investments and business relations with Russia; most of Moldova's energy is imported from Russia as well that creates limited sovereignty, especially in capabilities of shaping foreign policy. A diversification, especially including European countries, is needed to create a more sustainable and flexible operating environment.
4. Local media sector, on one hand, is not producing enough of good quality content and there is not enough support from civil society and development partners for the creation of strong and independent media outlets. On the other hand, the market is already heavily influenced by pro-Russian media outlets, so it is necessary to change that balance and create alternatives. For example, there are 290 TV channels in Moldova, 104 of them are coming from the Russian Federation and 201 from 292 are in the Russian language. Additionally, other sources and channels like Russian press agencies; Radio stations; Online news outlets and newspapers; Social media channels are used as platforms to spread propaganda and disinformation.
5. Finally, there is no coherence in Moldova on identity policy that has to be started to develop from a very young age in schools. Although the political plurality and minority rights always have to be protected in a stable democracy, the general identity crisis in

such areas as history, the local language, the role of minorities, the role of religion or in this case Russian Orthodox Church create cleavages in the society and might change foreign policy perception in the long term period.

The same or similar approaches could be applied to other countries as well, especially to those where Russia sees them as its sphere of influence. For instance, Russian influence right now is massive. In addition to previously mentioned channels, the possible Belarus unification with Russia in the near future can't be denied, so it is very important to look after the current situation. This action could be made not only to solve internal political problems of Russia by creating a new unified state but also to weaken the strategic position of the NATO Alliance, especially of the three Baltic States. Despite the fact that Belarus military forces are closely integrated with Russian forces, it doesn't mean that Belarus is no longer a sovereign state. The main narrative of Russia says that Belarus has to be together with Russia and that this union would be politically, economically and from the security perspective beneficial for Belarus. One interesting and unique pattern is that they are denying Belarus sovereignty, they are presenting that Belarussians do not have their own language – for the fellowships, Russian media is trying to prove that all citizens of Belarus are all Russian people. This is one of the main ideas of the Russian malign information – that countries like Belarus or Ukraine have no national identity and all Russian speakers (not even necessarily ethnic Russians) must be joined in one state.

In the case of Georgia, this country has not only to tackle and deal with the occupation of its territory but also to frequently respond to other hybrid attacks that are from the Russian Federation. The experts constantly distinguish Russian helicopters that enter the Georgian airspace without permission, for instance, on the 1st of October, 2018. The main message of these provocations is to lower the sense of security for Georgian citizens, especially those who still remember the war between Russia and Georgia in 2008. Russian side sees that provocations as a working tool and take these tools for granted since Georgia is not a member of the Alliance and no preventive political, institutional and security measures are adopted even on the national level. So we can see now that the aggressor can divide, interpret, multiply, and spread narratives in a completely different way.

Is there anything we can do?

From a historical point of view, experts tend to agree that national liberation movements or from the former Soviet Union in Latvia, Georgia, Estonia, Lithuania, and other countries are those examples that should be considered as the historical prototype of resilience. But today the effective resilience requires close cooperation between the civil society, non-state actors, governments and international alliances. It is also important to mention, that every country, first of all, has to create its own resilience system based on specifically for this country important and sensitive factors. Later, military alliances can create a joint system to improve security against different threats in different regions of the alliance.

What we can improve at the national level?

- *The psychological defence should be more reacting, that should ensure there will be no panic and the public will be aware of potential threats.* The public must know how to react to possible threats and accidents. For example, the Lithuanian Ministry of Defence has published a publication that defines how to react to the possible military, natural threats or any other extreme situations. Also, the governments should make clear which information sources are genuine and trusted in case of the real crisis and the reliability information must be backed to not allow to spread the disinformation sent from the foreign actors.
    - *Identifying all disinformation. Not only in the cyberspace but also on the physical way, soft power conferences, publications, and other physical events.* This can be done by looking for some keywords in the language of the enemy – it is essential to understand what an aggressor is using against you, while also constantly identifying national weaknesses are sensitive areas. This preventive measure can interrupt potential disinformation campaign.
    - *The baseline requirement for governmental resilience – sustainable, diversified and secure energy, transport, communication networks, etc.* It is a national responsibility, but some strengthening measures might be completed in cooperation with the regional partners. For example, Lithuania is putting a massive effort to become

independent from Russian energy import, so Lithuanians are building electricity lines with Poland and Sweden. This collaboration not only helps countries to become more independent and receive better prices in the energy market but also makes an energy sector more secure as these networks are under control of an ally from EU and/or NATO.

- *To raise the awareness countries may use big communication campaigns involving celebrities.* While it is necessary not create information bubbles and artificially hide existing problems, modern communication tools, such as using local, national and international celebrities who highlight the importance of participating in the politics to raise awareness against the fake news. Action like this could help to raise awareness among the younger generation and people who are not interested in current affairs and only look after entertainment TV shows, web pages and etc.

What we can improve on the NATO level?

- The prepared part is the most elaborate one, it includes *enhanced awareness* which means more and better intelligence sharing, strategic assessments, especially focus on particular sensitive regions as the Black Sea, Baltic Sea, Arctic, and North Atlantic. Also information environment assessments, which should be aimed to understand this information in the hostile narratives.
- One of the challenges – *the speed and quality of decisions that officials have to make*. NATO is a consensus-based organization, so our reaction time we have to understand will always be to some extent slower. Alliance also must adapt to *new challenges require new rules* to improve its resilience and quality of decisions. Quality can be significantly improved by institutionalizing and documenting hybrid threats on the political level. Additionally, existing grey zones must be reduced or if possible completely eliminated to prevent interpretation and fragmentation in the case-based situation.
- As being the largest and most advanced Alliance in history, the latest experiences, technologies, and innovations must be constantly shared on various levels. The members must develop joint *ideas and projects on the knowledge and solutions for identifying, tracking and sharing the type of threats*. It is hard for a single country or a single small company to create and refine massive technological projects, so NATO

countries and their companies can collaborate and support multi-national initiatives that could help to improve our defensive capabilities. Additionally, the Alliance must look and learn from other external examples that are indicating how hybrid threats are evolving and being applied.

- *NATO can and should improve its cybersecurity capabilities.* More and more technologies are becoming critical for all NATO forces and civil life, so the Alliance has to create a common defence system that could secure the infrastructure of the whole Alliance and its partners.
- An important task for Alliance is to *provide protection to the information field of its member states* – as it is now one of the major spheres of hybrid warfare. Creation of a system of counteraction to propaganda and disinformation could be made through cooperation with leading news agencies and the establishment of special structures that would track and assess the risks and threats in this area. The Alliance needs its own Global StopFake initiative, which, through cooperation with partner media, could expose false information to a large audience.
- Preventive actions against potential aggression could be strengthened by the *creation of the permanent system for assessing the situation in NATO member countries* regarding the areas and issues which are most threatened in hybrid contexts. In order to achieve such goal, the creation of special analytical multinational structure is needed. Its activities from the start should be directed to define the circle of threatened zones and issues, which could challenge the security situation and stability in each member-state of the Alliance (the weaknesses and sensitive problems, which could be used by the aggressor in his hybrid actions). Then permanent measurements of the situation in these areas should be implemented in order to give a signal about the potential hybrid attack in time.