10 YEARS EASTERN PARTNERSHIP Civil Society Forum

Funded by the European Union

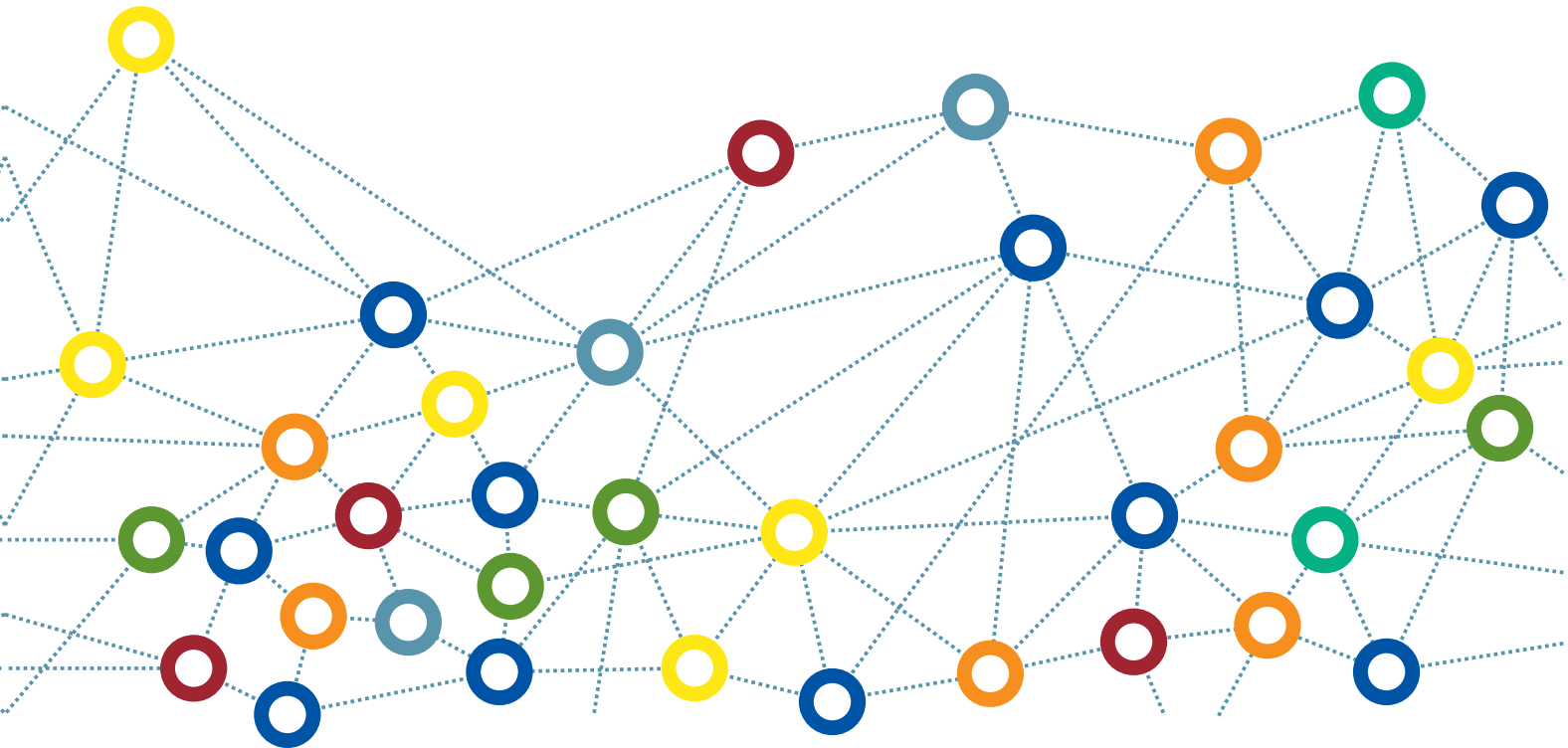
National Endowment for Democracy
Supporting freedom around the world

Ministry of Foreign Affairs of the Czech Republic

Countering Hybrid Threats: Stronger Role for Civil Society in Post-2020 EaP Roadmap

Policy Paper

TRANSITION
Transition Promotion Program



Countering Hybrid Threats:
Stronger Role for Civil Society in Post-2020 EaP Roadmap

Brussels, 2019

Authors:

Kakha Gogolashvili – Georgian Foundation for Strategic and International Studies (Georgia)
Mikayel Hovhannisyan – Eurasia Partnership Foundation (Armenia**)**
Elkhan Mehtiyev – Security expert (Azerbaijan)
Andrei Yahorau – Centre for European Transformation (Belarus)
Valeriu Pasa – WatchDog.MD (Moldova)
Viktor Ohiienko – Ukrainian Core (Ukraine)

Edited by **Kakha Gogolashvili**

The policy paper is produced in the scope of the project: "Developing deliverables on hybrid threats in post-2020 EaP roadmap – civil society perspective".

The project benefits from the support through the EaP CSF Re-granting Scheme and the Czech Republic Transition Promotion Program. The donors of the Re-granting Scheme are the European Union and National Endowment for Democracy. This report has been produced with the assistance of the European Union. The contents of this publication are the sole responsibility of the authors and can in no way be taken to reflect the views of the European Union.

CONTENTS

EXECUTIVE SUMMARY

The objective of the project, in the framework of which this policy paper was developed, is to promote the wider involvement of civil society in the policy area that can and should benefit from a multi-stakeholder approach through all stages of the policy cycle in the upcoming period in order to maximize the impact of joint actions and activities. The paper has an ambition to advise on how civil society should and could be involved in formulating, implementing and monitoring the future deliverables in the area of hybrid threats in the post-2020 Road Map for the EaP policy, including developing specific deliverables with concrete benchmarks for individual countries in a regional perspective. The paper feeds directly into the debate on the new EaP Road Map and structured consultation opened by the EU institutions, and builds directly on the recommendations from the EaP CSF policy paper "Advancing Eastern Partnership: 23 Civil Society Ideas for the Policy beyond 2020". It will be distributed to its target audience in Brussels, EU member states and EaP countries. Further advocacy and discussion with stakeholders in Brussels is planned during the 11th EaP CSF Annual Assembly on December 6, 2019.

The paper is a result of the joint research conducted by a team of experts representing CSOs from all six EaP partner states. The team conducted desk research and held consultations with stakeholders and experts in their respective countries. Each of them contributed to country reports and proposed recommendations for the development of cooperation on prevention and countering hybrid threats throughout the EaP area. The findings of the study covered the comparative analysis of hybrid threats in EaP countries, the response of the governments, cooperation between EU and EaP countries on countering hybrid threats, civil society engagement and, finally, the suggestions on the development of cooperation between EU and EaP partner states.

The research resulted in concrete recommendations for the governments of the respective countries, EU institutions and member states and for civil society, which is advised to intensify its engagement in countering hybrid threats and in developing a common response. Below are recommendations in short, a more detailed description of which can be found in the last two chapters below.

Recommendations for the Governments, EU Institutions and civil society

1. Each EaP government to establish a “hybrid cell” in which all information on hybrid threats is gathered.
2. Establish cooperation between the EU and the EaP country national structures countering hybrid threats.
3. Use Twinning facility and other financial instruments to support experience exchange and sharing between respective agencies.
4. The EaP Road Map beyond 2020 to envisage as a deliverable developing of an inventory of functions on hybrid threats, which the ministries and agencies of each country would include in their responsibilities.
5. EU itself is the process of building its integrated response mechanisms to hybrid threats. The EaP countries need to be involved in this process from an early stage.
6. Work on harmonization of the crisis response and in particular the hybrid threat response mechanisms with those already functioning in the EU.
7. To develop operational cooperation a focal point for each country and responsible EU agency to be appointed.

8. Organize trainings and regular meetings for reporting and exchanging information between focal points.
9. Establish intensive cooperation between EaP governments and EU-NATO Hybrid CoE, NATO CCDCoE, national centres in Member States. To create an "EaP section" in the Centre of Excellence, where experts from the EaP could do internships and contribute to the actual work of the Centre.
10. Capacity building for EaP countries' officials should envisage learning about the workings of ARGUS - the Commission's general alert system.
11. The sharing of experience on EU CERT to the EaP countries.
12. The Road Map to envisage assistance to EaP countries for the creation of similar response teams as EU has, share organizational experience of the Commission, on how ARGUS and ISAA operate and respond to crises.
13. As a deliverable the EaP countries be requested top adopt SOPs - the instructions for carrying out routine operations aimed at preventing and rapidly detecting and responding to a threat.
14. The inclusion of civil society in the Road Map as regards countering hybrid threats has become very important.
15. Inclusion of civil society participation in official EaP formats at all levels: representation of the EaP CSF in Ministerial (restricted form) meetings and Panels (full-fledged participation with the right and obligation to present views and participate in debates).
16. Include in the Road Map a plan for assessing civil society capacity and present a capacity development plan which would empower and allow civil society to become a capable and efficient counterpart and partner with official structures.
17. The Road Map to set measures to increase the motivation of the NGOs to engage, advise governments to establish a registry of organizations which will be invited and contacted regularly.
18. Each country to create a "trust group" of CSOs, which will be allowed to receive and work with the information which governments classify as "restricted" or "for internal use".
19. The Road Map to explicitly attribute to civil society an important role and the chance to influence the process.
20. The EaP states to be advised to actively use the findings of the civil society in the daily work and when possible outsource some actual tasks to the experts and active representatives of civil society
21. Civil society organisations form EaP countries and EU (Best if EaP CSF) to adopt a Strategy and Work Plan on countering hybrid threats.

INTRODUCTION

In this age of quarrel and hypocrisy…
Bhagavat Gita, 6-11

The Post-Truth era, first introduced by Ralph Keyes,[1] is not something resulting from a change in morality, ethics, or people's behavioural modus globally. Those changes happened several millennia ago, probably at the beginning of the historical Iron Age, or mystical *Kali Yuga*, as testified by ancient Sanskrit scriptures. The use of lies, which we now call disinformation, fake, distortion of the truth, etc., are well-known tools for conducting and supporting "quarrels", in this case, war. But why has the so called hybrid warfare today become so intense, penetrating practically every sphere of life, crossing the borders of any country and changing the minds of millions? Scholars say that the invention of the internet and the rapid advance of information technology has allowed "lies" to reach an ever wider audience. Indeed, the spread of social media, satellite and digital TV broadcasting has created fertile ground for the evil seeds of disinformation used by hostile actors for their own strategic aims. On the other hand, the internet and digital connectivity have become essential elements for the functioning of important industries, networks, financial institutions, energy networks, transport, etc. While these advancements increase the efficiency of the mentioned utilities, including their safety and security, they also increase their vulnerability to cyber-attacks.

The development of democracy, bringing transparency, the free movement of people, human rights, etc., also brings stability and increases human security in many senses. At the same time, the liberties and freedoms ensuring free movement, personal data protection, respect of property, freedom of speech and information present in a democratic country are effectively used by terrorists, hackers, and foreign spies to influence agents against the proper state and its population. Well-developed democracies, being resilient to social discontent, economic shocks, even the possibilities of kinetic warfare, become vulnerable enough to the hybrid tactics that are increasingly used against them by post-totalitarian and authoritarian governments; Russia, in particular. It is much easier to distort a country in transition, which obviously lacks all above-mentioned abilities to feel secure and resilient.

The classical understanding of the objective of the hybrid war is a weakening of the target country through the use of non-military subversive actions and preparing the situation for further kinetic war, followed by the occupation of a territory. In the modern reality, hybrid tactics are also used to distort the process of changes that the countries undertake in order to keep or bring the country under its influence. Philosophically, in essence, the action of forcing a country to surrender "spiritually" and ideologically is the same as being physically occupied. Both the classical and modern approaches of hybrid warfare are being employed against the EaP countries. In some cases, propaganda or other tools are used to prepare military aggression or to secure the occupation. In other cases, the main issue is to prevent the country from reproachment with the EU or NATO. Many different tools and methods are used to fulfill said goals.

[1] Keyes, Ralph (2004). The Post-Truth Era: Dishonesty and Deception in Contemporary Life. New York: St. Martin's. available at: www.hadinur1969.files.wordpress.com/2018/10/ralph-keyes-the-post-truth-era_-dishonesty-and-deception-in-contemporary-life-st-martin_s-press-2004.pdf

Since its establishment in 2009, the EaP initiative has made real progress in transforming and "Europeanising" Eastern Europe. All EaP countries depend on their relations with the EU. Georgia, Moldova and Ukraine signed and implemented Association Agreements; Armenia signed an Agreement on Cooperation and Enhanced Partnership; and Azerbaijan and Belarus are in consultations for deepening institutional partnership with the EU. Moreover, all of the mentioned states have significantly increased their trade with the EU; actively engaging in the dialogue and cooperation within EaP multilateral platforms. The EaP also aims at deepening regional cooperation between the EaP partner countries, which has also been largely achieved. It is fair to say that the EaP countries in many regards have similar goals and aspirations in wanting to deepen their relations with the EU, and some of them even aspire for EU membership as a long-term goal.

The growing attempts to destroy this trend by using military and non-military hybrid tactics has become an alarming reality and a challenge for those EaP state aspirations. The governments of the EaP countries have acknowledged the challenge and initiated development of a national response to the mentioned threats – creating institutions, legislation, and conducting anti-propaganda actions. But for the national response of EaP states to be able to outweigh the potent Russian hybrid machine, it is necessary to establish forms of cooperation (from exchanging information and jointly developing methodologies, to warning each other of potential attacks and cooperating on institutional capacity building) in order, together with the EU, to develop a solid common response.

EU EASTERN NEIGHBOURHOOD UNDER HYBRID ATTACK

Russia has long been using hybrid warfare tactics in the post-soviet space, but the world did not fully acknowledge the scale of its methods until the actions preceded by and following the occupation and annexation of Crimea. These methods include propaganda, spreading lies, active penetration by special forces, attacks on military objects using the civilian population, cyber-attacks on critical infrastructure, manipulation of criminal elements, actions of masked and disguised militarized elements; and afterwards – direct military intervention.[2]
Today, practically all EaP countries suffer from these and other types of hybrid threat. Among them:

Informational Threat. The country reports elaborated by the experts in the scope of this project provided information on concrete cases and showed that Georgia, Ukraine and Moldova are intensively subjected to *subversive propaganda* attacks. According to the messages, these countries are weak, corrupted, and dependent on the Russian market, lack the chance to be admitted into the EU and NATO, and see Russia promoting religious unity. The destructive messages are also reaching western partners and neighbours in the Eastern Partnership, messages which aim to diminish interest in deepening cooperation with said countries. Propaganda also affects Belarus, trying to convince its population of the impossibility of the nation surviving without Russia's support, destroying the idea of a Belarussian national identity and even its ability to continue as an independent state. Different types of propaganda have built up *anti-western messages* to discredit the EU and other Western partners' efforts and assistance to the EaP counties. EU integration is portrayed as a process containing the threat of the spread of liberal values and ways of life, which is, they say, contradictory to the traditional values in

[2] See: Kakha Gogolashvili. *European Union Facing Hybrid Threats*. Expert Opinion 121. GFSIS. 2019. p.4. Available from: www.gfsis.org/files/library/opinion-papers/121-expert-opinion-eng.pdf

Eastern European countries. To influence public opinion in all EaP countries, *disinformation*, consisting of a misinterpretation of facts, creates a false reality aimed at spreading untruths and confused perceptions and attitudes among the population. All EaP states suffer from daily disinformation. In many cases, this disinformation creates a bad and incorrect image of the neighbouring country and its intensions, and reduces openness towards others and the concept of developing fruitful cooperation. Disinformation is frequently used to incorrectly present the situation in conflict areas, adding to raising tensions, fuelling hate and reducing chances for reconciliation.

Destruction of the cyber space. Georgia and Ukraine are frequently targets of cyber-attacks. The first important cyber-attack against the Ukrainian energy system took place in 2011,[3] when around 200 thousand citizens were left without electricity. In 2017, Ukraine suffered its largest hacker attack on industrial facilities and government institutions (the NotPetya virus).[4] Several cyber-attacks have hit Georgia since 2008. The latest attack against the Georgian internet space took place on October 15-17, 2019, as a result of which, several thousand sites (private and official) collapsed for two days. Both countries are making efforts, largely successful, to counter the attacks, but need to further improve their cyber security. It can thus not be excluded that other EaP states, having many vulnerabilities, could also become victims to attacks in the future.

Anti-liberal groups supported by Russia or its proxies. Georgia, Moldova, Ukraine and Armenia face the threat of mushrooming anti-liberal groups, so called "defenders of traditional values", "patriots" and nationalists. These very much resonate Russian propaganda, imposing on public opinion the idea that western values are incompatible with national traditions. They attack both the governments and liberal/western-minded parties or groups in the country and never protest Russian interests. In Georgia, there have been cases of attacks on liberal media outlets.

Corrupting and financing of government officials and politicians to make them support Russian interests is widely seen in all EaP states. This form of subversion is especially damaging to Moldova, where many anti-western steps and decisions have been taken by politicians aligned with Russian interests. Financial tools have also been actively used to influence the electoral process in Moldova. Similar problems also face Ukraine, where we have seen corrupted media representatives acting against their own country's interests. In addition, many political activists are financed by Russia. Armenia's new government, which is trying to adopt European values, is also often attacked by corrupted politicians who frequently receive support (including financial) from abroad. Various tools and methods are used to influence political processes in the EaP states. Intervention in the electoral process is well-known, as happened in Ukraine and, especially effectively, in the Moldovan parliamentary and presidential elections. The methods are different and include cyber-attacks, information theft from certain sites, financing pro-Russian parties and groups, financing and influencing supporters, etc.

Supporting pro-Russian/anti-western mass media and NGOs. In all EaP states, there are internet or printed editions of news and analytical materials displaying and spreading the Russian official point of view on what happens inside and outside the country. They deal with many themes and try to influence public opinion by providing "alternative views". "Independent" NGOs, financially supported by Russia, organise conferences, workshops, outreaches (lectures and seminars in regions and rural areas), public diplomacy, etc. with a similar purpose of supporting Russian viewpoints and criticizing the West and EU values.

---

[3] See at: www.jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/

[4] See: Andy Greenberg. T*he Untold Story of NotPetya, the Most Devastating Cyberattack in History*. Available from: www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

So called **"active measures"** involve agents of influence working with vulnerable groups in all EaP countries to gain their support of Russia's policy in the region. Easing **procedures** for obtaining **Russian citizenship** ("passportization") is equally employed in all EaP states.
Economic and energy blackmailing are also frequently used against practically all EaP states, be it Georgia, Moldova or Ukraine, where embargoes have been introduced on several occasions, or Armenia and Belarus, which are frequently forced to take certain decisions under the pressure of their economic and energy dependence on Russia.

Many other forms of hybrid attack are being used, not yet clearly identified and some in the phase of planning and development. Indeed, it is not a major issue what kind of attack is threatening a country, but the overall realisation of the fact that any attempt to create an independent foreign policy that is not compatible with Russian interests will be prevented and, on continuation, punished. Any of the mentioned tools can be used in the future against any of the EaP states.

NEED FOR A JOINT EFFORT IN COUNTERING HYBRID THREATS

The nature of the hybrid threats the EaP countries are facing, is in many aspects identical by content as well as by source. There are obvious differences that can be traced while analysing the content in each country separately. So the question arises, should the EaP states treat their security challenges separately or does the rationale suggest it would be better to join forces? Meanwhile the particularities of each state are better addressed individually, the potential advantages that come from cooperating on countering common hybrid threats are indeed high.
Table below, which is based on the narratives developed by the country experts lists the objectives (not exhaustively) of the Russian hybrid strategy towards EaP countries. It demonstrates that the aims of the hybrid warfare conducted by Russia against Moldova, Georgia and Ukraine (GMU) are almost identical. For example, any EaP country is subject to subversion as regards their European aspirations, democracy building, national unity, sovereignty and independence (political and economic), resisting separatism and resolving conflicts. Therefore, notwithstanding the differences in relations between a concrete EaP country and Russia, there are still many aspects where EaP countries could have an interest in joining efforts, exchanging information and helping others to increase their resilience to the hybrid threats. At present, there is no platform for the cooperation of EaP countries[5] in the mentioned field, nor between the associated EaP states, who are facing practically identical threats from the same source.

[5] Save occasional meetings in the framework of the Panel on Security, CSDP and Civil Protection

Table. Objectives of the Russian hybrid strategy for EaP countries

	Armenia	Azerbaijan	Belarus	Georgia	Moldova	Ukraine
Hybrid Threat Objective						
Weakening of State Institutions						
Weakening Democracy						
Weakening Defense Capacity						
Questioning EU values						
Reducing Support to EU Integration						
Opposing Euro-Atlantic Integration						
Corrupting government and politicians						
Influencing elections						
Weakening national identity						
Strengthening pro-Russian sentiments						
Destabilization						
Political polarization						
Affecting critical infrastructure						
Trade diversion						
Justification of occupation						
Affecting economy						
Supporting separatism and protracted conflicts						

What have the EaP countries been doing to counter the existing threats?

Ukraine developed certain measures to counter the hybrid threats, but the legal mechanisms to limit a particular hybrid threat within the country are lacking, among them Security Sector Integrity. A reform of the security institutions would allow for the creation of a unified coordination model to counter the hybrid threats. The lack of a media strategy to counter hybrid threats is also a problem. A large and influential media does not always oppose the manifestations of hybrid warfare.

In 2018, the Parliament of the **Republic of Moldova** approved a law prohibiting the retransmission of political or military news and broadcasts from the Russian Federation. However, the propaganda inserted in Russian entertainment shows is increasing. The National

Information Security Strategy approved in 2018[6] includes priorities to increase the capacity to respond to cyber-attacks and misinformation, but the strategy is superficial and does not define a clear source of hybrid threats.

The legal basis for countering hybrid threats in **Georgia** is as yet undeveloped. A draft strategy was recently submitted to Parliament. It is necessary to empower institutions legally with concrete competencies in this regard. The strategy will define changes in laws and the division of competencies among institutions. At present, the Ministry of Internal Affairs formally coordinates the work on internal security issues. The Ministry of Foreign Affairs is responsible for strategic communications and for building informational resilience. It also cooperates with relevant structures of partner countries and IOs. The State Security Service conducts work on the fight against terrorism, the cyber-security of state institutions, and on preventing subversive activities by penetrated groups. The Ministry of Defence (MoD) works to prevent hybrid threats to the country's defence system, including the cyber security of its services. The overall political coordination of all the elements is still not secure.

Belarus lacks any comprehensive policy to counter hybrid threats. In 2016, it adopted a new military doctrine which defines internal threats as "mechanisms for the forceful overthrow of objectionable political regimes by provoking internal armed conflicts." The Conception of Information Security aims at preventing hybrid threats in the information sphere. The adopted documents and measures are not fully compatible and promote the perception of the West as the main source of threats.

There is no special body in **Azerbaijan** involved specifically in information gathering, sharing and assessing hybrid threats. Some of these activities are being carried out by different security agencies, such as the defense intelligence, state security service or foreign security services, which focus on foreign subversive activities as well as on local actors, such as religious groups. They also deal with the protection of energy infrastructures. Among the measures undertaken on cyber security, special organs – the Electronic Security Service, State Agency on Special Communication and Information Security, have been established to ensure communications security and defense from cyber-attacks Increased attention is being paid to securing the state services' internet sites and the computer systems of vital energy and transportation bodies.

NATO, Azerbaijan, Georgia and Turkey cooperate in the form of training and exercises on addressing hybrid threats to energy infrastructure throughout the region. **Armenia** is developing a new National Security Strategy in line with current developments, geopolitical realities and emerging threats to security (including hybrid). The Concept of Information Security and Information Policy of 2017 and Cyber Security Strategy adopted in 2017 establish a framework for government measures to counter hybrid threats. The Information and Public Relations Centre of Staff and Digital Armenia Foundation are the most efficient bodies in tackling the respective foreign propaganda, yet Armenia still lacks a comprehensive governmental approach to addressing cyber threats[7]. The US-based Defense threat reduction agency has trained many Armenian scholars and practitioners on biological threat reduction, while NATO's IPAP program has trained people in civil emergency preparedness.

The EaP countries have not established any direct bilateral or multilateral cooperation on countering hybrid threats among themselves, but they have already had discussions and exchanged experience in the framework of the Eastern Partnership. The only relevant forum for such discussions is the EaP Panel on Security, CSDP and Civil Protection, where, under EU

[6] www.rm.coe.int/3-moldova-strategy/168097eceb

[7] Nerzetyan, A. 2018. Information Security or Cybersecurity? Armenia at a Juncture Again. EVN Report. [online] Available at: www.evnreport.com/economy/information-security-or-cybersecurity-armenia-at-a-juncture-again [Accessed on 22 October 2019]

guidance, EaP government officials exchange views on elements of hybrid threat, in particular, propaganda and disinformation. The EU brought elements of hybrid threat to the EaP multilateral format earlier by including co-operation on security issues, especially in the area marked as A10 in the EaP roadmap for 2012-2103[8] - the fight against cybercrime, which has as specific objectives: defining strategic priorities on cybercrime; developing tools for action against cybercrime, and strengthening EaP country capacities to implement action against cybercrime. Another field of cooperation that can be considered as related to the hybrid threats is A11 - Civil Protection, which aimed at developing partner countries' civil protection capacity for prevention, preparedness and response- mainly to natural and manmade disasters. Here, the relevant Flagship Initiative under Platform 1, set up in 2011, is worth noting. All the above mentioned topics at that time were matters of internal security for the EU. The same road map suggested the creation of a CSDP Panel to discuss international security issues and step up cooperation on issues of international security among EaPs. Later, in 2017, with the elaboration and adoption of the comprehensive program for EaP multilateral cooperation, "20 Deliverables for 2020" (Agenda 2020), the issue of cooperation on hybrid threats was further specified in Deliverable 12 (security), with the aim of increasing "the resilience of the Partner Countries to security threats, including hybrid threats…" strengthened "through stronger cooperation in the area of security and disaster risk management." [9]

Another important type of hybrid threat – disinformation and propaganda, is addressed in the Agenda 2020, Deliverable 3, namely, by strengthening Strategic Communications in the EU and EaP countries. Monitoring of the implementation of the named deliverable in 2018 has shown some tangible results. Indeed, it was noting that "Communication campaigns are ongoing in all Partner Countries. Particularly comprehensive communication campaigns have been launched in Georgia ("EUforGeorgia") and Ukraine ("Moving forward together")."[10] As a result, 60% of the population in EaP countries have developed a positive attitude to cooperation with the EU.

The specific objectives addressed "areas of illicit firearms trafficking and cybercrime to make them more resilient to hybrid threats, including cybersecurity, to mitigate CBRN risks of criminal, accidental or natural origin, and to be better prepared to prevent conflicts and manage crises." The majority of these areas were relevant to the risks that the EaP countries are facing today, but the Agenda was still not gathering all the stock of hybrid threats into one basket of cooperation. The same report assesses the implementation of Deliverables[12] (security, including hybrid threats) and refers to the topics attributed to countering hybrid threats only in relation to the cyber security strategies, adopted by Georgia, Moldova and Ukraine.

Overall, the co-operation among EaP countries on countering hybrid threats is only at the initial stage, while such threats are growing, threatening not only the security of the Partner states, but also European integration in the region. In a number of documents, the EU has recognised the need to establish closer cooperation in the engagement of the EaP countries and to assist them to become resilient to the mentioned threats. On the basis of its conclusions of July 6, 2017, the Council of the EU offered (under Action 18 of the Joint Framework for Countering Hybrid Threats) to run surveys of the vulnerabilities and needs in partner countries which Moldova and

[8] Brussels, 15.5.2012 SWD (2012) 108 final Joint Staff Working Document: Eastern Partnership Roadmap 2012-13: the multilateral dimension.

[9] Brussels, 9.6.2017 SWD (2017) 300 final JOINT STAFF WORKING DOCUMENT Eastern Partnership - 20 Deliverables for 2020 Focusing on key priorities and tangible results. Available from: www.ec.europa.eu/neighbourhood-enlargement/sites/near/files/eap_20_deliverables_for_2020.pdf

[10] See at: www.ec.europa.eu/neighbourhood-enlargement/sites/near/files/20_deliverables_2020_state_of_play_monitoring_sept_2018.pdf

Georgia completed in 2019[11]. Future EU assistance to the mentioned countries, as well as to other EaP states, may be shaped in accordance with further analysis of the survey results. Without doubt, the results will be embodied into the EaP Road Map beyond 2020, which puts a greater focus on concrete actions to increase resilience and the ability of EaP states to counter hybrid threats.

DEFINING ELEMENTS FOR THE EAP ROAD MAP BEYOND 2020

When the EaP was established 10 years ago, a clash of geopolitical interests nor wider security challenges were well acknowledged neither by the Eastern partner states or the EU. 10 years on, it has become evident that security in the Eastern neighbourhood is challenging the further progress towards the EaP goals set in the Prague Declaration (2009). The EU Global Security Strategy marked this new stage in perception of the role of security in the European integration process and put a spotlight on guarding and supporting the resilience of partner states in its neighbourhood.[12] The security needed to be indivisible and to be guarded in a collective manner. This last is relevant not only for the states, but for societal actors, in our case for civil society first of all. At this stage, it is well understood that civil society cannot be separated from security related problems and should act and contribute everywhere possible and affordable for it to do so. The state is often unable to counter hybrid threats without the active support of society. Civic participation is becoming critically important in countering information attacks on social networks, debunking and restricting the spread of fake news, mobilizing civic opposition to attempts to organize social unrest, working to develop national media and cultural content, strengthening national identity, etc.

Each EaP government could be advised to establish a "hybrid cell" in which all information on hybrid threats is gathered. The hybrid cell should have analytical staff and the ability to act as an early warning source unit when a potential threat is detected. It is important to establish cooperation between the EU and the national structures countering hybrid threats. The EU Twinning facility could be used to support experience exchange and sharing between respective agencies.

The Road Map could also envisage working on developing an inventory of functions, which the ministries and agencies would include in their responsibilities. As different functions in different countries are conducted by different agencies in cases of emergency, it may be difficult to establish rapid operational contact with each other. The inventory would help to identify a necessary agency not by its name or affiliation, but by the registered function assigned to it.

The EU itself is actually in the process of building its integrated response mechanisms to hybrid threats, and the EaP countries need to be involved in this process from an early stage. It is important to harmonize the crisis response and in particular the hybrid threat response mechanisms with those already functioning in the EU, as well as those yet to be introduced in order to guarantee a quality and effective common response.

To develop operational cooperation, a focal point for each country and responsible EU agency (EEAS would be the most appropriate) needs to be introduced. The can serve as a direct contact as regards to any question related to planned meetings, exchange of information, liaison needs,

[11] JOINT REPORT TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL AND THE COUNCIL on the implementation of the Joint Framework on countering hybrid threats from July 2017 to June 2018. p.11. Available from: www.eeas.europa.eu/sites/eeas/files/joint_report_on_the_implementation_of_the_joint_framework_on_countering_hybrid_threats_from_july_2017_to_june_2018.pdf

[12] EU Global Security Strategy. p 25. Available from: www.eeas.europa.eu/archives/docs/top_stories/pdf/eugs_review _web.pdf

etc. The Road Map should also envisage trainings and regular meetings for reporting and exchanging information between focal points. In the best case scenario, the focal points would be placed in the national hybrid cells of each EaP State.
Some EaP countries have already established cooperation with the EU-NATO Hybrid CoE, NATO CCDCoE, and with national centres, but more institutionalised cooperation is needed to create an "EaP section" in the Centre of Excellence, where experts from the EaP could do internships and contribute to the actual work of the Centre.
Capacity building for EaP countries should envisage learning about the workings of ARGUS - the Commission's general alert system. No EaP country has an expanded team which can be present in all governmental institutions and deal with cyber and information security. The sharing of experience on EU CERT would be important for the EaP countries. The Road Map could also envisage assistance to EaP countries for the creation of similar response teams.
The organizational experience of the European Commission, in particular on how ARGUS and ISAA operate and respond to crises, can help the countries to establish the same kinds of system of integrated inter-agency responses to crises or security threats.
The EaP countries should adopt SOPs - the instructions for carrying out routine operations aimed at preventing and rapidly detecting and responding to a threat
The inclusion of civil society in the Road Map as regards countering hybrid threats has become very important.
We suggest to reinforce civil society participation in official EaP formats at all levels, the representation of the EaP CSF in Ministerial (restricted form) meetings and Panels (full-fledged participation with the right and obligation to present views and participate in debates and make recommendations). Further, the Road Map should, to our mind, develop a plan for assessing civil society capacity and present a capacity development plan which would empower and allow civil society to become a capable and efficient counterpart and partner with official structures. Such a capacity-building plan should also envisage permanently updating relevant civil society organizations (EaP CSF, national platforms and other registered groups) about new threats, methods used to counter them and problems that challenge counteractions.
The Road Map should set measures to increase the motivation of the NGOs to engage, and should advise governments to establish a registry of organizations which will be invited and contacted regularly when governments have news to share or are seeking their advice or participation. Such CSOs can even create a "trust group" which will be allowed to receive and work with the information which governments classify as "restricted" or "for internal use".
The civil society organisations in EaP countries are already largely engaged in the media monitoring, debunking propaganda, analysing cyber threats, working with vulnerable communities, etc. So, the EaP governments can capitalize on and use their experience and effectively employ their findings, expertise and widely outsource the growing tasks lightening the burden for official structures.
The Road Map should explicitly attribute to civil society an important role and the chance to influence the process. Civil society action can further be detailed in the Work Plan that follows adoption of the Strategy. In the best-case scenario, the Work Plan will be adopted and renewed every two years at the EaP CSF Annual Assembly.

STRATEGY FOR THE ENGAGEMENT OF CIVIL SOCIETY IN COUNTERING HYBRID THREATS

While the governments need time for defining common goals and planning joint actions, creating cooperation formats and models of interaction, civil society could take the initiative and promote this cooperation from its own perspective. Civil society organizations from the EaP countries, actively supporting the Eastern Partnership and European integration, are better positioned to unite their efforts to counter destructive hybrid threats. Many organizations from EaP countries have already started working together to understand the nature of security threats and vulnerabilities, doing joint research, and organizing roundtables and discussions on hybrid threats

An overall objective of the Strategy should be increasing security in the EaP countries and their ability to resist hybrid threats coming from any source and to any area of public life, economy or politics. The Strategy should have a medium/long-term perspective (7-8 years), with possibilities for regular adjustments and adaption to the rapidly changing environment.

I. The Strategy should serve the following specific objectives:

a. Defining the type of threats the EaP countries face and could confront in the future;
b. Defining areas where the vulnerabilities can be targeted by an adversary;
c. Identifying tasks for civil society groups and non-state actors to counter the hybrid threats at both the national level and EaP-wide;
d. Setting provisional and long-term benchmarks for the success of the civil society activities;
e. Introducing measurable indicators a) for evaluating the dynamics of the security environment (in relation to the expansion/reduction of the space for hybrid threats); b) for the progress achieved by civil society in terms of the real impact of their action on the reduction (positive case) of the hybrid threats in EaP area and, in particular, in each EaP country.

II. The strategy should contain analyses of:

a. The security environment in the EaP area;
b. The types and sources of hybrid threat by country and in common;
c. The resources the countries have to counter the threats;
d. The readiness of the institutions and resilience of the state;;
e. The relations between the EaP states and willingness and possibilities for joint action
    i. that the states do together.
    ii. that civil society groups from the EaP countries already do together.
f. The cost/benefit of uniting efforts of civil society from EaP countries.

III. The Strategy should establish a set of principles for cooperation of EaP civil societies on countering hybrid threats.

a. A threat or attack against any EaP state is a matter of concern and reaction from all EaP CSOs.
b. Only objective and well-proven facts can be shared between CSOs.
c. Cooperation should be based impartiality and solidarity.
d. Differentiation in the multilateral cooperation formats can be applied to issues specifically relevant only for some states and not others.

e. Joint ownership should mean that CSOs from all EaP countries should seek the commitments of their governments to support and take some financial burden of activities carried out within the Strategy.
f. Information on deficiencies or the weakness of official structures on any side shared by a CSO, and which if widely covered can result in, damage to the security of the named state shall only be used for internal discussions and for the elaboration of mutually beneficial recommendations.

IV. Areas of CSO cooperation:

a. Cooperation and active engagement with the state and governmental institutions, European structures and EU institutions, international organizations.
b. Elaboration and consideration of national and joint reports on existing and potential hybrid threats.
c. Adoption of joint declarations and the carrying out of advocating campaigns to bring to the attention of the governments, EU or IOs issues related to weak response to a new or already existing hybrid attack or threat.
d. Conferences, discussions and roundtables with the participation of official bodies responsible for preventing and countering hybrid threats. Such events would ensure proper and similar understanding of problems by civil society and governments, and politicians will be able to communicate more effectively with civil society to demonstrate their position regarding said issues.
e. Projects uniting the efforts of experts, teachers and activists for: producing quality analyses (monthly, quarterly, and annual) of dynamics in the sphere of hybrid threats in the EaP area; training and developing the capacity of CSOs and government officials in the area of hybrid threats, covering wider topics and issues directly or indirectly related to hybrid warfare.

V. Final and Institutional provisions.

a. The Strategy should propose (a) format(s) facilitating joint actions and the further engagement of civil society in countering hybrid threats.
b. Different suggestions for the setup of a special group for countering hybrid threats come from almost all country experts participating in this study. One option is a crosscutting subgroup ("Civil Society Hybrid Cell"), which would unite representatives of all five groups and maintain links between each of them.
c. Actions may be taken at different levels, so relevant cooperation formats should be created at the national (on the basis of EaP CSF National Platforms), forum (on the basis of the EaP CSF), extra forum (EaP CSF + independent NGO groups and coalitions working on hybrid threats) and extra NGO (extra forum + independent experts) levels.

The EaP CSF Annual Assembly should adopt the Strategy, after consideration and revision by all six CSF EaP national platforms, EaP CSF delegates (including EU delegates), members of bilateral civil society platforms set up between EU and EaP Associated states. The process of the review should envisage wider participation by experts in the field and NGO coalitions working on hybrid treats