ENC ANALYSIS

Ensuring Security in Ukraine and Eastern Europe: New Formats for EU/NATO Cooperation with Ukraine

July 2018

Authors: Samuel Doveri Vesterbye, Mykhailo Gonchar, Andreas Marazis, Vitalii Martyniuk

ABOUT THE AUTHORS

Samuel Doveri Vesterbye

Managing Director of the European Neighbourhood Council (ENC)

Mykhailo Gonchar

President of the Centre for Global Studies (Strategy XXI)

Andreas Marazis

Head of Research for Eastern Europe and Central Asia
European Neighbourhood Council (ENC)

Vitalii Martyniuk

Head of the International Programs of Centre for Global Studies (Strategy XXI)

Ensuring Security in Ukraine and Eastern Europe: New Formats for EU/NATO Cooperation with Ukraine

Europe faces a multitude of threats today. Apart from the obvious military provocations on its borders, the European Union (EU), its partner countries and the North Atlantic Treaty Organization (NATO) face a range of hybrid threats including disinformation campaigns that are bitterly impacting its citizens' sense of unity. Ukraine is on the front line to counter these hybrid threats from the East, more specifically from Russia. Therefore, both the EU and the Alliance are vital partners for Ukraine in its security efforts. The joint interest is, of course, to settle the conflict peacefully and to strengthen the sustainability of Ukraine's future security work with the long-term goal of regional stability, peace and prosperity.

Ukraine doesn't have the means to respond unilaterally to Russia's aggression, especially if it is intensified. At the same time Kyiv has proven itself to be a valuable partner for NATO's past and ongoing missions, while pushing for closer integration with the EU by implementing the Association Agreement. Despite reforms taking place in both political and economic areas, the reality remains that even with enough successful security sector reforms, the prospect of Ukraine becoming a NATO member still remains a distant reality. Therefore, the next step should be based on results and the prospect for deeper and more developed EU-NATO cooperation, as well as Ukraine's role within a stronger EU architecture for the neighbourhood.

Towards this goal the joint EU-NATO Declaration is only the first step. Two out of the seven key areas are focused on cyber security and on strengthening the defence capacities of the Eastern and Southern partners. It is not a coincidence that in the June 2017 progress report on the implementation of the common set of proposals, endorsed by both EU and NATO Councils alike, a special reference was made of the fact that ten out of the forty-two actions are dedicated to countering hybrid threats, including cyber-attacks. Strategic communications has a central role in conveying messages of unity and solidarity towards the partners, increasing the visibility of both organisations and countering disinformation.

However, both the EU and NATO need to be reminded that the situation in Donbas might change rapidly and Russia can intensify its aggression against Ukraine. Therefore, Ukraine should reach as high a level of its resilience as it can due to enhanced cooperation with the EU and NATO.

To discuss and investigate the possibilities for increased EU-NATO cooperation in relation to Ukraine and the field of security with an accent on cyber security and strategic communications, the European Neighbourhood Council (ENC) and the Centre for Global Studies (Strategy XXI), with support of the NATO Information and Documentation Centre in Ukraine, organized the two-day conference entitled "New Formats for NATO and EU

Cooperation with Ukraine" on 30-31 May 2018 in Kyiv[1]. Based on the results of the conference, this report examines the EU-NATO cooperation in relation to Ukraine in the fields of cyber security and strategic communications, which have the objective of further embedding the country's security.

EU-NATO Enhanced Cooperation and Ukraine

At the NATO Summit in the new Headquarters in Brussels on 11-12 July 2018, the EU-NATO Enhanced Cooperation celebrated its second anniversary. For these past two years, cooperation between the EU and NATO has increased in all fields, from hybrid threats and cyber security to maritime cooperation. Deterrence, resilience, cyber security are a few of the buzzwords that continuously reoccur throughout the many statements and official documents.

The question is whose capabilities and resilience are the EU and NATO trying to strengthen? There are some who seek to draw a firm line between NATO's allies in Central and Eastern (CE) Europe and its partners just beyond its border. However, deterrence in CE Europe is inextricably linked with NATO policy in partner countries like Georgia, Ukraine and Moldova. Moreover, the official position of the Alliance was declared in the Bucharest NATO Summit Final Statement in 2008, as a cornerstone of NATO policy towards Ukraine and Georgia: "NATO welcomes Ukraine's and Georgia's Euro-Atlantic aspirations for membership in NATO. We agreed today that these countries will become members of NATO".[2]

The three progress reports that were released in December 2016 following the endorsement by the North Atlantic Council and the Council of the European Union on the common set of proposals highlighted the importance of the Black Sea region and the need to assist EU partners in the Western Balkans, and across the Eastern and Southern neighbourhood.

The Baltic States and Poland in the meantime, due to the growing Russian military resurgence, requested and were granted NATO combat forces on their soil – three to four thousand soldiers – to be stationed on a rotational basis. Indeed, multinational battle groups to the East of the Alliance are now fully operational, while at the same time NATO is stepping up its efforts against cyber-attacks and hybrid threats. In September 2017 Dragon-17, a biannual defensive military exercise, was completed in Poland with the participation of various NATO forces from Poland, Lithuania, Latvia, Germany, United Kingdom (UK), Slovakia, Italy, Bulgaria and Romania as a response to the Russian-led Zapad-17 military drill. The drill was focused on countering hybrid warfare tactics, similar to the ones used in Ukraine, as well as cyber-attacks. It is worth mentioning that Ukrainian and Georgian forces participated in the exercise as well.

[1] https://geostrategy.org.ua/en/component/k2/item/1473-post-reliz-novi-formati-spivpratsi-nato-i-es-z-ukrayinoyu

[2] https://www.nato.int/cps/en/natolive/official_texts_8443.htm

One could argue that the exercise is a substantial example of successful military coordination and that strengthening the states that lie between NATO and Russia is primarily an economic and political task for these states themselves; including Ukraine. It is about providing assistance in order for Kyiv to be able to address its security challenges. For example, after the annexation of Crimea, Russia dramatically increased its military presence and capabilities in the Black Sea region. There are currently six submarines, which can carry out nuclear warfare and reach Western and Northern European states. This requires increased cooperation between the EU, NATO and Ukraine on strengthening security in the Black Sea. A 2017 ENC internal report demonstrates the rapidly decreasing Black Sea naval capability of NATO countries like Turkey, pointing towards the increased necessity for NATO-Turkey-Ukraine cooperation and coordination in such areas. Solidarity, unity and cooperation among EU and NATO members would send a stronger message than any military hardware.

It is very important that the EU and NATO have a joint assessment of the situation, which will provide a common understanding of the threats, and in turn will make it possible to formulate a common goal. Both organisations are focused at the moment on strengthening their deterrence mechanisms. The idea is that EU-NATO cooperation will support their partners in their effort to increase their resilience, as well as to grow stronger politically and economically, in order to be able to defend themselves from internal, hybrid and external threats.

In the framework of EU-NATO Enhanced Cooperation there are currently three pilot countries: Moldova, Tunisia and Bosnia & Herzegovina, and three key areas of interaction: ammunition storage and safety, cyber security and strategic communications. These cooperative efforts will strengthen the resilience of the non-member partners against potential aggression, and will also contribute to their reform process. The pilot phase has been undergoing and the expected results are likely to benefit other partner countries immensely – Ukraine included. The third progress report on the implementation of a common set of proposals endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017[3], state that information exchange, including informal staff-to-staff political consultations on the three pilot countries (Bosnia and Herzegovina, Republic of Moldova and Tunisia) also takes place for Ukraine, Georgia and Jordan.

During the above mentioned two-day high level conference in Kyiv, the potential of an increased EU-NATO cooperation in relation to Ukraine, in the fields of cyber security and strategic communication and with the objective of further embedding the country's security, was widely discussed for the first time. It was a key opportunity for policy-makers in Kyiv and for NATO and EU officials based in Ukraine and Brussels to discuss new formats of cooperation between the EU, NATO and Ukraine in the framework of the EU-NATO Enhanced Cooperation focusing specifically on cyber security and strategic

[3] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

communication.

Focus on key areas

According to the third progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils[4], the key spheres of EU-NATO cooperation, which should be spread on their cooperation with Ukraine, are: countering hybrid threats; operational cooperation including maritime issues; cyber security and defence; development of defence capabilities; defence industry and research; exercises; building of defence and security capacities; and political dialogue.

One of the seven common priority areas for the two organizations (EU and NATO) according to the declaration is to support Eastern and Southern partners' capacity-building efforts. It is not a coincidence that on the 14 June 2017 progress report on the implementation of the common set of proposals endorsed by EU and NATO Councils, special reference was made to the fact that ten out of the forty-two actions are dedicated to countering hybrid threats, including cyber-attacks. Strategic communications also has a central role in conveying messages of unity and solidarity towards partners, increasing the visibility of both organisations and countering disinformation.

Countering hybrid threats remains of key importance with 20 out of the 72 current proposals for EU-NATO cooperation focused in this area, which is of vital importance for Ukraine. The security challenges for Ukraine and the entire Eastern Partnership region influenced the content of the EU-NATO cooperation. Despite the implementation of both the NATO-Ukraine Platform on Countering Hybrid Warfare and the development of the Draft Platform Working Program, it is necessary to deepen cooperation in this area with participation of the EU through active involvement of Ukraine into the work of the European Centre of Excellence for Countering Hybrid Threats *(*Hybrid CoE*)* stationed in Helsinki, Finland. This is possible through the establishment of an Eastern European office of the Hybrid CoE in Kyiv, Ukraine. This will help show how relevant the war in the Donbas has become for wider European security concerns. The Eastern European office can provide an opportunity to engage in meaningful dialogue and to address the challenges associated with hybrid warfare, using Ukrainian and other experiences as a practical example. This would enhance EU-NATO-Ukraine cooperation in countering hybrid threats, facilitating improvements in early warning and situational awareness, strategic communication and messaging, crisis response, resilience, and cyber defence and energy security, which was defined in the third progress report as further steps for enhancing EU-NATO cooperation.

Two out of the three key areas of interaction in the pilot phase are on cyber security and strategic communications. The Heads of State and Government participating in the meeting of the North Atlantic Council in Brussels on 11-12 July 2018 stated: "We face

[4] https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_06/20180608_180608-3rd-Joint-progress-report-EU-NATO-eng.pdf

hybrid challenges, including disinformation campaigns and malicious cyber activities."[5] That is why in Ukraine – but not only there – these two key areas require further attention.

Strategic communication is mentioned in the third progress report as a primary sphere of trilateral cooperation. Under the auspices of the EU Delegation, NATO is chairing a donor coordination group for the defence and security sector, and is closely cooperating with the EU Advisory Mission to Ukraine on strategic communications and other issues in Ukraine. Ukrainian governmental bodies continue to develop strategic communication, but remains to be integrated, structured and defined in the nation's national legislation. Moreover, Ukraine needs clear mechanisms of strategic communication in different spheres and can develop them with the assistance of NATO as it was defined in the Strategic Communications Partnership Road Map between the National Security and Defence Council of Ukraine and the NATO International Staff.

Cyber security remains important for EU-NATO cooperation, which includes a set of common measures. At the same time, the EU assists Ukraine due to its Advisory Mission and NATO assists Ukraine through its Trust Fund on Cyber Defence to develop Ukraine's capabilities. This two-way assistance needs to be coordinated in correspondence with the EU-NATO cooperation in the cyber security sphere.

In all its previous papers on security issues, Strategy XXI emphasized the importance of the finalization of Ukraine's entrance in the NATO Energy Security Centre of Excellence in Vilnius, Lithuania, and transferring this practice to the NATO Strategic Communications Centre of Excellence in Riga, Latvia, and NATO Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia.

Strategic Communication

Getting the right message out in a conflict such as this one, waged by Russia against Ukraine, has proven to be challenging not only for the authorities in Kyiv but also for NATO and the EU.

Several projects have been implemented on behalf of the EU in order to support Ukraine in its attempt to tackle some of these issues, such as the EU Mythbusters twitter feed, the Disinformation Review and the Russian Language News Exchange Centre in Prague-- where there are journalists from different countries sharing news stories in the Russian language and helping each other in their investigations and reporting, making sure that a substantial story can be picked up and shared more widely.

The relationship between NATO countries in Europe and their neighbourhood deserves special attention that goes beyond government relations as strategic communication also concerns non-governmental actors. Western Europe, as a society, has much to learn from

[5] https://www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en

their Eastern neighbours, both when it comes to youth engagement, civil society participation and civic mobilisation in the face of external threat.

In line with its report on Threats to Stability in Wider Europe, the European Neighbourhood Council (ENC) recommended to increase links between civil society organisations, while improving dialogue among ordinary citizens living inside the EU and across the Eastern Partnership area. Ukraine, Georgia and Moldova must be engaged, both on a civil society and governmental level, with their neighbours across Europe in terms of value campaigns, information sharing, involving societies in the monitoring of the events taking place in the EaP countries, trainings and cooperation through EU-UN led mechanisms in protracted conflict areas. This is particularly relevant, as European and NATO countries, and their citizens, necessitate a transparent, cooperative and uniform understanding of threat.

When it comes to EU-NATO cooperation in Ukraine on strategic communications, prior to the Warsaw Summit, the sides resorted to elements of coordination through regular meetings, exchange of training plans, sharing expertise in various communication disciplines and the delivery of joint trainings. At the same time, NATO needs Ukrainian experience to develop strategic communication in the fighting area in the East of Ukraine.

Ukraine is developing strategic communication, but it should become one of the key areas of cooperation and be perceived in Ukraine not as a public relations campaign, but as strategic planning. The best way for Ukraine to utilise the expertise and the resources that both the EU and NATO offer is by incorporating a concrete strategy for strategic communications into its national strategy. The basic principle is that the recipient country must have a strategy, while the donors align their efforts according to the priorities of the strategy. Thus, assisting the Ukrainian government to develop a StratCom strategy should be the first step for the EU and NATO, before the implementation of any collaborative project.

Cyber Security

Cyber security faces similar challenges as strategic communication in Ukraine. Ukraine has many skilled hackers and cyber experts. They lack, however, full-fledged coordination and interactions with international partners. For example, EUAM Ukraine cooperates with the Cyber police of Ukraine and the NATO Liaison Office in Ukraine, as well as with the Security Service of Ukraine and the National Cyber Security Coordination Centre at the National Security and Defence Council of Ukraine. The last one is determined by the Cyber Security Strategy of Ukraine as a national coordinator in this area. Meanwhile, proper coordination remains an important issue as it does not single-handedly depend on what kind of strategies or policies they develop. Equally, the funds and efforts by donors have a limited impact, as long as coordination on behalf of the host country remains sub-optimal.

However, in the cyber security sector the picture is more optimistic. The NATO Trust Fund on Cyber Defence, which is headed by Romania, played a significant role so far in providing Ukraine with technical, training and advisory support. The purpose was to enable the development of Ukraine's own cyber security incident response teams and its strictly defensive CSIRT1-type technical capabilities, including laboratories to investigate cyber security incidents. In 2015 five training courses were delivered by Estonia, which is one of the eight contributors in this Trust Fund, to the Ukrainian side as in-kind contribution, focusing on cyber security incident response team related training, strategic-level training (e.g. cyber policy and strategy) and defensive cyber security development.

In July 2017 the first phase of the trust fund was completed based on Ukrainian needs, while the second phase is still in its early stages and remains under negotiations. The main recipients were the Security Services of Ukraine (SBU) and the State Security Service for Communication and Information Protection (SSSCIP). When it comes to technical support, two incident management centres were established within the SBU and the SSSCIP. Equipment and the software necessary to protect the information infrastructure of the Ministry of Foreign Affairs of Ukraine have been delivered. NATO's Cooperative Cyber Defence Centre of Excellence studies the situation in Ukraine and cooperates with the Ukrainian actors responsible for cyber security issues.

Additionally, the EU, through the Eastern Partnership Panel on Common Security and Defence Policy (CSDP) provides not only Ukraine, but all six EaP members, with a forum to exchange information. EU member states and EaP partners provide their insights and ideas on how to develop their cooperation; basically to coordinate what the member states are doing, what the Eastern partners consider a priority and what the EU can contribute. The EUAM provides assistance to the Cyber police of the National police of Ukraine and tries to coordinate all donors' activities in this regard.

The framework strategy for cooperation in cyberspace should be applied globally, and cyber security measures should be well coordinated at the multilateral level. Improper interagency coordination in the field of cyber security and the absence of a concrete strategy for strategic communications may discourage and confuse the donor community. In future EU-NATO progress reports, Ukraine could potentially be in the spotlight if the authorities in Kyiv keep up the reform pace. An emphasis on interagency coordination would subsequently create the right conditions for potential EU-NATO cooperation to unfold in the areas required, including strategic communications and cyber security.

Recommendations

Taking into account the current development of the EU-NATO cooperation (as well as European and Euro-Atlantic integration of Ukraine and their prospects) it is desirable to implement the following recommendations, prepared as a result of the above mentioned 2-day conference in Ukraine:

For further development of EU-NATO-Ukraine cooperation in general:

- Combine European and Euro-Atlantic integration of Ukraine into one case, since this complex of internal reforms is smaller compared to the process of integration into the EU. Simultaneously, carefully coordinate Ukrainian needs with the new developments of NATO coordinated EU defence initiatives, including PESCO and the European Intervention Initiative.
- Deepen cooperation between the NATO Representation Ukraine, the NATO Liaison Office and the NATO Information and Documentation Centre, and the EU Delegation to Ukraine and the EUAM to better coordinate activities in Ukraine within the Donor Coordination Mechanism as well as involve the country into the process of NATO-EU security cooperation.
- Consider Ukraine not only as a recipient but also as a contributor of security in Europe to establish regional security system under EU and NATO auspices with Ukraine at the core.
- Encourage NATO Centres of Excellence to assist Ukraine in facing Russian aggression, especially COEs focusing on cyberspace (Estonia), energy security (Lithuania), and strategic communication (Latvia).
- Continue the work of the NATO-Ukraine Platform on Countering Hybrid Warfare and expand it on Ukrainian non-governmental think tanks, which facilitate research in this area.
- Establish an Eastern European office, based in Kyiv, of the European Centre of Excellence for Countering Hybrid Threats *(*Hybrid CoE*)*, which is stationed in Helsinki, Finland.
- Use EU and NATO experience to develop democratic control over the security and defence sector of Ukraine and to enhance further trilateral cooperation in this dimension.
- Utilise EU-UN models and EU experience in dealing with conflict resolution for Ukrainian conflict areas.

For EU-NATO-Ukraine cooperation in Strategic Communication:

- Assist Ukraine in developing and adopting its national strategy on strategic communications and sectoral mechanisms to implement this strategy.
- Initiate joining of Ukraine into the NATO Strategic Communications Centre of Excellence which would help Ukraine to develop all necessary acts on strategic communication and deepen cooperation with the Alliance in this sphere.
- Create new links between Ukrainian and Western European think tanks to develop stronger human security, unity and exchanges of ideas or best practices, and develop youth contacts on issues of common values and security in Europe. The cooperation between ENC and Strategy XXI serves as a useful example of think tank cooperation.

For EU-NATO-Ukraine cooperation in Cyber Security

- Complete setting-up a clear and working coordination system in the cyber security sphere to fully implement the Cyber Security Strategy of Ukraine, to draw all national actors, including non-governmental, and make NATO, EU and other assistance more addressed and effective.

- Use the EU and NATO experiences and practices to create a wide national cybersecurity certification scheme, develop a Blueprint for how to respond to large-scale cybersecurity incidents and crises, deepen the public-private partnerships and strengthen research.
- Initiate the joining of Ukraine into the NATO Cooperative Cyber Defence Centre of Excellence that would help Ukraine to implement the best practices and deep cooperation with the Alliance in this sphere.
- Enhance cooperation in strengthening cyber security in Ukraine to prevent and neutralize a possible Russian intervention during the upcoming presidential and parliamentary elections in Ukraine.