CONCLUSIONS AND RECOMMENDATIONS

CFSP and Serbia's Accession to the European Union: What Next?

6 December 2018

The main focus of the expert conference "Common Foreign and Security Policy and Serbia's Accession to the European Union: What Next" was on Serbia's alignment with the Common Foreign and Security Policy (CFSP) in the context of EU accession negotiations and Chapter 31 (Common Foreign, Security and Defence Policy). Issues such as other challenges that directly affect the formulation of the CFSP with respect to security and defence in Europe, such as hybrid threats and cyber security, were also discussed at the conference.

The conclusions and recommendations are based on the debates held during the conference and they reflect views and opinions voiced during the debates. However, they do not necessarily reflect the views of each participant. The person responsible for the content of this document is Igor Novaković, Director of the International and Security Affairs Centre - ISAC Fund. Also participating in the drafting of this document were Miljana Ivković and Mirjana Đorđević.

Chapter 31 and Serbia – How to Achieve Alignment?

- Even though Chapter 31 has not been opened yet, Serbia is very active in implementing some elements contained therein. Serbia has signed an operational agreement with the European Defence Agency and has been participating in the system of EU Battlegroups since 2016. Serbia is also the first candidate country to have applied for participation in the Permanent Structured Cooperation (PESCO) within the Common Security and Defence Policy (CSDP) of the EU. Serbia has passed the Law on Restrictive Measures, which is harmonised with the UN principles on the use of restrictive measures and which lays the basis for the country's participation in EU's restrictive measures. Acceptance of a comprehensive approach to security was particularly highlighted, as it also requires involvement of the civil component that is primarily reflected in Serbia's progress in developing a system for participation in EU's civilian missions. Serbia also excels as the leading candidate country in the Western Balkans in terms of its participation in EU military missions, which reaffirms its determination to share and protect European values.
- The lack of a screening report for Chapter 31 is still an obstacle to Serbia's progress in the EU accession process. The Common Foreign and Security Policy is a relatively new concept whereby the EU has tried to affirm itself as an influential international actor in foreign and security affairs, particularly amid continuous competition among global powers. To that effect, the EU needs a strong and effective CFSP and thus it is not surprising that the EU is concerned over a drop in Serbia's alignment with the CFSP although EU member states do recognise and welcome the development of cooperation with Serbia in certain areas (migration, arms control, CSDP, PESCO).
- The drop in the alignment of Serbia's foreign policy with that of the EU (54%) has an impact on the EU's decision not to open this chapter yet. In the 2018 European Commission Progress Report, Serbia's progress in this area was assessed as 'moderate'. Some panelists from Serbia were of the opinion that to boil everything down to imposing sanctions on Russia would be an oversimplification of the overview of the alignment process, which also entails alignment with all foreign policy positions and actions of the EU, as well as adoption of necessary legislation. However, the drop in the alignment with EU's foreign policy approach is a major obstacle in the accession process since the CFSP is seen as 'the least common foreign policy denominator' for all member states and full alignment must be achieved until the time a country is admitted to EU membership.

- When it comes to Serbia's approximation to the CFSP, an increasingly higher emphasis on the security concept is noticeable. Serbia views security sector reform as a segment of reform that must be implemented by the whole society irrespective of EU membership prospects if it wants to attain a certain level of functionality and development in conditions of peace.
- EU membership is indeed a foreign policy priority of the Republic of Serbia and Serbia is exerting every effort towards achieving that goal, which has also been defined as a national interest of the Republic of Serbia in its National Strategy. However, Serbia is also committed to the issue of results of the dialogue between Belgrade and Priština, and it expects comprehensive and sustainable result and solution to be achieved. Serbia's interest in this respect does not only refer to Chapter 35, but also to Chapter 31 and other chapters. Serbia has no hidden agenda or strategy in that regard. It is in Serbia's national interest not to oppose the position of those countries that are helping it protect its national interest in the context of the Kosovo issue. From that perspective, the drop in the alignment with the EU foreign policy following the outbreak of the Ukrainian crisis is the result of a complex situation Serbia is facing.
- The EU accession is more than just a technical process as it implies a political choice, as well. The example of Montenegro, which opened this chapter in 2014, but is still awaiting its closure despite having complied with all the legal requirements, shows that a political dimension is crucial for closing this chapter. The Common Foreign and Security Policy is a broad area, with one of its fundamental issues being the relationship between the EU and the Russian Federation. The drop in Serbia's alignment with the EU foreign policy approach makes it more difficult to encourage EU member states to continue the enlargment policy. Quite a few EU member states believe that postponing Chapter 31 and waiting for all other chapters to be closed is not the best strategy. EU member states are aware of the complex situation Serbia is faced with, and they are ready to help stimulate a discussion and find the best possible solution. There is an open communication between Serbia and the EU, as well as Serbia's open explanation of the reasons for the lack of alignment with EU positions in individual cases. However, the understanding that the EU has demonstated in this context does not mean that it approves of such action or finds it acceptable.
- Positive examples of alignment (Belarus, North Korea, Nicaragua) show that progress is possible. Progress should be more convincing and sustainable, which means that Serbia would have to demonstrate through specific action that EU accession is its national interest rather than just a strategic priority.

Cyber Security and Hybrid Threats – New Dimensions of Security for Serbia and Europe

- Hybrid security means every coordinated and synchronised action that deliberately targets democratic states' and institutions' systemic vulnerabilities through a wide range of means - political, military, civil, economic, and information. Hybrid threats are also defined as activities on the border between war and peace, whose aim is to influence the decision making process at different levels of authorities.
- According to NATO and Russian definitions, hybrid threats include military and non-military as well as covert and overt means, ranging from disinformation, cyber attacks, economic pressure and deployment of paramilitary formations to the use of regular units. Both state and non-state actors may be involved. However, state actors have increasingly been using non-state actors as intermediaries. Users of hybrid threats can be highly flexible, i.e. their method of threats is being constantly adjusted, like the one used by the Islamic State, for instance.
- Mass communication, widespread social networks, availability and a lower price of some advanced systems make hybrid threats more certain than before. Moreover, there is a new tendency of some states using hybrid action against their own citizens.
- When considering an appropriate response to hybrid threats, some problematic issues may arise. In suppressing disinformation as a hybrid threat, the state must form its own counter-narrative. The question is, however, how this counter-narrative is going to be formed, how credible it is going to be and where it should stop.

- As for economic influence and control, as another form of hybrid threat, the question is how to keep all the benefits of free movement of capital and still maintain a certain level of control or public awareness of the dangers that hybrid threats may pose to social development.
- When considering hybrid threats, the information domain is also singled out, as information technologies have revolutionised business operations and society in a broader sense. Hence, it is no wonder that most e-government programmes/processes/projects are key reform projects in the world today, and Serbia is no exception in that regard.
- Cyber security that refers to the protection of critical infrastructure differs from the classical concept of cyber security. Cyber security has revolutionised the security concept for several reasons: a. The cyber space knows no physical borders. Cyber incidents can spread very fast to the whole world; b. Cyber incidents have a serious disruptive potential. Although the so-called 'Cyber Armageddon' is not real, some major cyber attacks have taken place in the recent past, for instance a cyber attack on Estonian systems in 2007, which caused a temporary malfunction of the financial system in that country; c. Cyber incidents affect the economy. "Cyber crime has become an economy of its own, due to cooperation that knows no borders."; d. There is a problem of attribution. Despite the use of intelligence work, a definite answer to the question "Who performed the attack?" cannot be given. For all these reasons, states are developing not only defensive but also offensive capacities in the cyber domain.
- At the international level, there are efforts towards creating a normative framework in the domain of cyber security. The main 'arena' is the United Nations that brings together groups of government experts around the idea of developing international norms. It has been agreed that international norms governing classical relations between states should apply in the cyber space, as well. However, their further operationalisation or adjustment is slow, which shows the complexity of this process that is politicised due to the current relations between states.
- The EU pays major attention to cyber security. In its 2016 Global Strategy for the Foreign and Security Policy, the EU defines cyber security as one of five foreign and security policy priorities to be achieved within the Common Foreign and Security Policy. In 2017 Jean-Claude Juncker ranked cyber security as the fourth most important issue, ahead of migration, which illustrates the importance that the EU attaches to this issue and the intensity with which the EU has been dealing with this security threat. The EU has developed one of the most robust systems to tackle this issue at the level of policy, security and economy, which is also important for Serbia as a candidate country.
- Serbia is trying to respond to key challenges in the approach to e-service security and to harmonise with global trends. In the past few years, Serbia passed the Law on Information Security and the Law on Critical Infrastructure that Serbia was lacking, because in the development of electronic services the question arose with respect to the infrastructure that the country had relied upon. The strategic and normative frameworks are in place and Serbia is now working on developing good practices and preventing and exercising responses to incidents.
- The public administration believes that all systems in the Republic of Serbia are secure, which means that, apart from applying all relevant international standards, these systems are closed and that there is also a closed data network within the public administration. The state Data Centre has been set up. Serbia has centralised information security and everything that has to do with e-government, with a system of direct accountability to the Serbian Prime Minister. This enables better coordination as compared to earlier times when the approach to and treatment of this area used to be institutional.
- E-services and portals are vulnerable systems due to the vulnerability of the Internet space itself. Serbia will also have systems that will give citizens access to their own personal data, which will be significant in the context of transparency and safety.
- The army and the police are not the only actors in the cyber space. The competent Serbian authority in this domain is the Ministry of Trade, Tourism and Telecommunications. A Coordinating Body for Information Security has been set up as an advisory body that reports to the Government. This also body includes the Ministry of Defence, the Ministry of Interior, security agencies, i.e. all major decision makers in the state administration.

- The Republic of Serbia has been implementing activities towards developing competent human resources capable of responding to relevant risks in this domain. There is an important ongoing project of developing a curriculum for master studies in information security at the universities of Novi Sad, Belgrade and Niš. Universities cooperate not only among themselves and with international universities, but also with the private and NGO sectors. This will strengthen the society's resilience to cyber threats.
- Some believe that two major hybrid threats in Serbia are disinformation, i.e. 'spinning' as a soft form of hybrid threat, and economic pressure, i.e. efforts to excercise control over the means of communications and information.