The regional expert workshop and conference
„Countering online radicalization in the context of cyber security“

Belgrade, Saint Ten hotel, 16 – 18 April 2018

## Background information

### Countering online radicalization

Following the great increase of incidence of radicalization, especially among the youth, in South East Europe and Europe in general, in recent years, together with the increase of level of terrorist and violent extremist activities, significant progress has been made in efficiency and coordination of responses to it – prevention and countering violent extremism (P/CVE). Relevant national authorities (law enforcement services first and foremost), international and regional organizations and initiatives, academia, civil society – everyone has their role to play, and the mutual coordination is of key importance.

After such an extensive experience, it can safely be said that radicalization is only rarely and exceptionally happening fully under the influence of online content. For a person to get really radicalized, online hate speech, terrorist and violent extremist propaganda has to somehow be anchored in that person's life experience and situation. The "offline" socializing plays a crucial role more often than not, in particular in the final stages of the path to radicalization.

Despite all of this, online terrorist and violent extremist propaganda, often very professionally and skilfully executed, is by no means to be underestimated. It led, directly or indirectly, hundreds or even thousands of individuals from a more or less regular life somewhere in Europe to the faraway foreign battlefields, or lured them into becoming terrorist or violent extremist propagandists themselves.

The more and more widespread digital "culture" of fake news, hate speech, very strong and statements and "analyses", often totally divorced from reality (including numerous conspiracy "theories") confuse thousands of ordinary people, youth in particular. When they come to question parents', school and government authority and reliability (which is fully normal "growing phase"), young people very often get confused, making them an easy target of "vendors of hate" of various ideological and political hues.

Instead of offering "counter-narratives", we have collectively graduated to trying to offer alternative narratives. Or even more simply, we as governments and societies simply have to offer our youth positive perspectives, positive alternatives to any and every form of exclusion, hatred, violence and extremism.

Obviously, it is far easier to say it than to do it effectively. This conference intends to give its contribution in that direction.

**Cyber security**

These days, the whole world is becoming more and more digitalized. Same goes for commerce, functioning of public administration and all governmental services, media, international relations, culture and entertainment. In fact, all aspect of contemporary life and especially human relations are already fully digitalized or are being digitalized in an increasing degree.

This has been fully recognized by the European Union, which is in this area at the global forefront. The EU Cyber security Strategy was adopted in 2013, underlining the importance of cyber resilience, reducing cybercrime, development of cyber defence policy capabilities including industrial and technology resources. The Network Information Security Directive was adopted in 2016, while in September 2017 the European Commission adopted a cybersecurity package with new initiatives aimed to improve EU's cyber resilience, deterrence and defence. One of the proposals was to strengthen the European Union Agency for Network Information Security (ENISA).

South East Europe and in particular the Western Balkans is not lagging behind. First and foremost, technological and economic gap between the Western and WB6 is far shallower in digital world than in general economy. The importance of digitalization and cyber security has been recognized by the national governments in the region. The Western Balkans Six (WB6) Leaders endorsed in July 12, 2017 the Multi-annual Action Plan for a Regional Economic Area (MAP) aiming to promote trade integration, introduce a dynamic regional investment space, facilitate regional mobility, and create a digital integration agenda. Trust and security and digital services, as one of the policy areas of the MAP, incorporates activities that aim to Enhance Cyber Security, trust services and data protection. A Stocktaking and Need Assessment report is prepared by RCC Secretariat where major policy gaps and needs, including assistance through bilateral or regional projects are identified – detailed information on Cyber Security, trust services and data protection can be relevant for the purpose of this assignment.

In 2008, the SEECP Ministers of Foreign Affairs adopted a Common Declaration regarding the strengthening of cooperation in combatting cybercrime, agreeing to step up efforts at national and regional level in cyber security. The SEECP Bucharest Summit Declaration (June 2014) underlined the importance of intensified cooperation in the field of cyber security, as one of the most important challenges region is facing. It figured prominently on the agenda of 2017 Trieste Summit of the Berlin Process, and the same will be the case with the 2018 London Summit.

Digitalization or "going online" offers great opportunities for sending, getting, gathering, and analysing information and therefore speeding up and facilitating journalists' work, scholarly research, business, public administration functioning and other areas of human work and life. At the same time, it greatly facilitates terrorist, criminal and other malevolent activities, such as:

- malicious cyber-attacks on virtual and digitalized "real life" critical infrastructure (ranging from messing up with civil status registries of citizens, disclosing classified information and sensitive

personal data to disrupting the functioning of air, railway and road traffic and electricity supply systems)

- trade in illicit merchandise (weapons, drugs, human beings, stolen art etc.) through “Darknet”, “regular” Internet or other electronic means

- money laundering, fraud, extortion, and other financial criminal activities, including financing of terrorism and violent extremism

- terrorist and violent extremist propaganda and misuse of social networks and online media for online radicalization.

The academic community and responsible authorities have started recognizing the gravity of such threats at national, regional, European and global level, at both legal and practical plan. Much more, however, remains to be done, and a real and full view of the existing situation is the first step towards defining, planning and executing measures to improve prevention and countering of such illegal activities, threatening to seriously harm societies in WB6 and Europe as a whole.

**Connection**

Countering online radicalization and cyber security efforts are two areas of work inside the whole area of security that are rarely seen and discussed together.

One of the main purposes of this event is to bring together these two aspects, see the connections between them, and try to give some recommendations for action for the main stakeholders – relevant national authorities first and foremost.