Opening speech by RCC Secretary Majlinda Bregu
at the High-Level Cybersecurity Conference
"Cybersecurity challenges and opportunities in the Western Balkans"
Tirana, 9 July 2024

Madame Deputy Prime Minister Balluku,
Excellencies,
Dear Guests,

Welcome to the second edition of the RCC High-Level event on "Cybersecurity Challenges in the Western Balkans," this time in Tirana. There were many reasons why we decided to move this important high-level discussion among policymakers and the international community from Brussels to the Western Balkans, and specifically to Tirana. I will mention just one: Albania, one of the countries in the Western Balkans and a NATO member, has been under continuous state-sponsored attacks that steal sensitive personal information and disclose it publicly.

Our security landscape is rapidly evolving. Migration isn't just a flow of people; it's a national security issue. Brain drain is now a security threat, not just an economic issue. We face climate change, natural disasters, and the ever-growing menace of cyber threats. We are permanently under attack. Now, our personal lives can be easily violated and invaded at any moment by a cyberattack. The internet is less and less Spotify and more and more WannaCry, as we are still unclear about how destructive cyber weapons actually are. Today, we are threatened even by a single message we open on our mobile phones, an email we do not read carefully, or one careless click of "OK" when browsing the internet.

With 5.2 billion people worldwide having access to the internet and 66.2% of the population using it for over 2 hours and 23 minutes daily, cybersecurity is the most important topic of today, and not a threat of the future. Cybersecurity is no longer merely a matter of national security but has emerged as a global security challenge. There are 800,000 estimated cyberattacks annually worldwide, and we are not ready to combat this powerful weapon.

1. **The cyber-skills and talent shortage continues to widen at an alarming rate.** There is a 3.2 million job gap in cybersecurity, and this situation will not improve in the next two

years. 52% of public entities state that a lack of resources and skills is their biggest challenge when designing for cyber resilience.

2. **There is a clear need to revisit the national strategies and make them fit for a cyber-age.** More and more, the EU is articulating and moving toward regulated digital technologies, including AI development, which risks exposing citizens to data security violations and harmful content. We have witnessed that realistic image- and video-generating models are aggravating the disinformation problem. The number of organisations that maintain minimum viable cyber resilience is down to 30% worldwide.
3. **Cyber-attacks have become an imminent threat to our democracy.** In recent months, there has been a rise in Russian-linked disinformation sites misleading the audience and influencing the election process in the EU. They look like regular print news websites, but the content is AI-generated with a pro-Russian narrative, intentionally misleading users, especially in Germany, France, and Poland. Over 70% of Europeans regularly encounter fake news. The frequency with which we encounter fake news and its potential to influence the way we think, how we vote, and what we believe has made it an important issue in society today. Publishing and sharing of fake news have become easier in an increasingly digital world, and social media plays a large part in this. 83% of EU citizens consider fake news a problem for democracy.

The challenges in the Western Balkans do not differ much from those in the EU, and in some areas, we are more vulnerable:

- The Western Balkans have seen a significant increase of 40% in cyber incidents in the past year. In 2023, more than 1.2 million personal records were exposed due to data breaches in the region.
- Ransomware attacks have surged by 200% over the past two years in the Western Balkans. The average ransom demand in the region is around €150,000, with some organisations paying over €1 million to recover their data.
- 75% of businesses in the Western Balkans reported phishing attacks in the last year.
- 60% of cloud environments in the Western Balkans are found to have critical vulnerabilities due to misconfigurations, and over 50% of organisations in the region have experienced a cloud-related security incident in the past year.

Some worrisome figures captured by our Balkan Barometer include:

- The top security concerns among Western Balkan citizens are migration, war fears, cybersecurity breaches, and disinformation.
- Nearly one in two (41%) citizens is worried about potential cyberattacks.
- 57% of Western Balkan citizens expressed concern that there has been an increase in fake news in their economy during the last year (Macedonians and citizens of Bosnia and Herzegovina are concerned the most, with 71% and 65%, respectively).
- Nearly half of our citizens (47%) believe that disinformation spreads hatred and divisive opinions.
- Social media and journalism are often blamed for fake news, with 46% pointing fingers at social media and 44% at journalists.

- There is a lack of digital literacy—42% of citizens consider it the main problem. For example, 69% of respondents from Albania do not use online services due to a lack of digital skills.
- Cyberattacks have drastically reduced citizens' trust and confidence in using the internet—from 51% in 2022 to 21% now.

As with all security threats, cybersecurity is not an isolated issue of one economy but a cross-border concern, as a cyberattack on the critical facilities of one economy can affect other economies in the region. Cybersecurity is at the forefront of our security agenda, and the data from the Western Balkans region is telling: we are in dire need of prioritising awareness, knowledge, and skills, aligning legislation with the EU, and joining forces with the EU on several fronts.

Last year we launched this high-level dialogue, and we are pleased to witness real progress on the main takeaways from that meeting, such as:

- Digital skilling has been prioritised by all Western Balkan economies in their National Reform Agenda as part of the Growth Plan.
- The ID-Wallet is now not just a proposal of the RCC but is envisaged by the EU as an area of accession to the EU Single Market. Moreover, it will not simply remain at the level of the Western Balkans but have a clear perspective of accessing the EU ID Wallet.
- The RCC, with the support of the EU, is establishing a platform to identify the real needs of the Western Balkans in cybersecurity and develop a regional approach to respond to these needs. The work on identifying needs will build on the existing security platform under IISG.
- There have been concrete developments in aligning Western Balkan legislation with the EU acquis, especially with regard to the harmonisation with the NIS 2 Directive.
- Lastly, cybersecurity has been strongly envisaged as a predominant area in the Common Regional Market's second iteration. As part of CRM 2025-2028, a stepping stone for integration into the EU Single Market, cybersecurity is featured as one of the priorities of digital transformation. It started with very few elements on CSRTs four years ago, and now we will work together on policy reforms that will entail, but not be limited to:
    - Facilitating processes that prepare and support the Western Balkans to integrate into the EU cybersecurity certification framework. This process will be phased to mirror the respective processes in the EU.
    - Maintaining the regional dialogue on cybersecurity that would enable a regional response as well as support capacity building in partnership with TAIEX and other specialised organisations.
    - Developing AI together and aligning the respective legislation with the EU acquis.

Let me conclude with a few key takeaways:

1. **International Cooperation**: Cyber threats do not respect borders. The EU and the Western Balkans must continue to strengthen international cooperation, sharing intelligence and best practices with global partners.

2. **Digital Europe Programme**: This programme is a great investment opportunity in digital capacities for all Western Balkans. Unfortunately, the access of the Western Balkans to this programme does not include cybersecurity. Extending the DEP to include cybersecurity should not be seen as a financial opportunity for the region but as a matter of security.
3. **EU Cybersecurity Certification Framework**: The framework for ICT products enables the creation of tailored and risk-based EU certification schemes. The scheme will apply on a voluntary basis EU-wide and focus on certifying the cybersecurity of ICT products in their lifecycle. Integrating the Western Balkans into such a scheme would benefit the increased cybersecurity of ICT products in the region.
4. **ID Wallets**: Part of the Growth Plan, as well as regional activities, will make a difference in the lives of Western Balkan citizens. Strong links and synergies between cybersecurity certification and ID Wallets and managed security services signal the high need for integration into EU policy from the onset and the need to work hand in hand with the EU on this.
5. **Inclusion in the ACTING Project and Cybersecurity Skills Academy**: The EU should explore the potential of including the Western Balkans in the ACTING (advanced European platform and network of cybersecurity training and exercises centres) project and the Cybersecurity Skills Academy. On the other side, the Western Balkans should consider this a top priority and make a real contribution to joining this structure.
6. **Public-Private Partnerships**: Governments and private sector entities must collaborate closely to enhance cybersecurity measures and respond effectively to incidents. Private companies should be as involved in the development of digital skills as governments. With more companies moving towards digitisation and cloud adoption over traditional data security solutions, many now have more acute cybersecurity needs.
7. **Investment in Cybersecurity**: Adequate funding for cybersecurity initiatives, including research, infrastructure, and workforce development, is essential. This includes supporting small and medium-sized enterprises, which are often targeted due to their limited resources.

Embracing all-inclusiveness and fostering a participatory society is paramount in our endeavour to implement cybersecurity measures across the Western Balkan region.

International and regional security and stability in cyberspace are intertwined. Cybersecurity is a perspectives exercise. Technology speaks volume on opportunities but also on risks.

There is an urgent need to regulate the digital world as the stakes of effecting human rights in the digital world are under severe attack.

Now, I have the pleasure to invite Deputy Prime Minister of Albania, Madam Balluku to join the stage for her welcoming remark, followed by our dear friend in arm, Madam Anna Vezyglou, Deputy Head of Unit for WB at DG Near

Madam Balluku, the floor is yours.