Check Against Delivery

RegionalCooperationCouncil

Co-funded by the European Union

Talking Points by the RCC Secretary General *Majlinda Bregu*

at the
EU-Western Balkans Regulatory Dialogue meeting, Brussels 30 June 2023

Dear Ministers,
Dear Director Koopman,

Although we joined this conference at mid-day, this doesn't stop me from welcoming all the participants at this high-level event organised in close partnership with the European Commission that aims to explore the frontiers of knowledge and the unknown, converge experts' insight experiences, and hopefully explore cutting-edge solutions to the complex challenge of cybersecurity.

There are many developments that attract greater attention from the Balkans where conflict is never unthinkable than the big challenges we all share.

Unfortunately, while in the Balkans we feel like an escalation of conflict is always about to happen, a new form of crime that has little to do with the use of force, the cybercrime, is perpetrating our economies. Albania is still experiencing cyber-attacks following a serious attack from Iran in 2022.

A moment like this reminds you that this is the real warfare. Your institutional system can go to a complete shutdown, your data can be deleted, your public services disrupted ,the lives from birth to school, marriage to death and a NATO member classified information can be thrown into disarray.

The same happened in Montenegro, when we were jointly organising a SEE Foreign Affairs Ministerial. For days we sent emails to MFA of Montenegro to fine tune the details of the event, but there was no response from their side. Then we tried the old version - gave them a call. The response from Montenegrin colleagues on their silence towards our emails caught us by surprise: their email system was shut down and they sent the relevant information via fax. As most of the organisations that are so into technology, our fax machine was unplugged for years and was merely part of the inventory.

What do these stories have in common? Cybersecurity is not merely a buzzword. Cyber-attacks call for a greater partnership in the cyber sphere. If national security is indivisible at a global level, actions and consequences are interlinked too.

Dear ladies and gentlemen,

Digital transformation in the Western Balkans has become a key driver of economic growth and societal changes.

The interconnectedness of our societies, economies, and governments has brought forth unprecedented opportunities, but it has also exposed us to significant risks.

- 60% of Western Balkans citizens use internet over 2 hours daily
- One in three citizen (32%) consider that cybersecurity threats in their economy will increase in the upcoming years.
- Top three risks associated with the use of digital tools are: safety and wellbeing of children 47%; cyber-attacks and cyber-crime 41%; and security of online payments 30%.

Cybersecurity is not solely a technical issue, but a multidimensional challenge and it requires a combination of technological, legal, cooperation and educational measures.

RegionalCooperationCouncil

Co-funded by the European Union

1. Cyber-attacks are borderless – a joint regional approach to ensure cybersecurity in the region, in line with EU standards, has become a must. WB economies need robust legal frameworks that facilitate cooperation and information sharing amongst WB economies and WB-EU, but a high level political commitment to cybersecurity reforms comes First.

Creating a unified framework and strategies for cyber governance, risk management, and incident response; harmonizing cybersecurity regulations; and promoting cross-border collaboration and cooperation to combat cybercrime are prerequisite for a safer digital environment within WB. The governments should dedicate sufficient resources and attention to cybersecurity measures to protect the region's critical infrastructure, businesses, and citizens.

2. Education and awareness are equally vital components of a comprehensive cybersecurity strategy. We went around the region asking about disinformation and whether anything about it is learned through schools and school curricula. Hardly so, was the answer.

From basic cyber hygiene practices like strong passwords and regular software updates to recognising phishing attempts, or understanding social engineering techniques are becoming a must for our educational systems.

Unfortunately, the region is lagging behind when it comes to digital skills. Only 35% of WB citizens possessed at least basic digital skills, while in EU the average is nearly 54%.

3. Lastly, we should work together against a common enemy. Cybersecurity is one of those areas where stronger collaboration between public and private sectors is pivotal to strengthening cybersecurity. The reality we are facing in the region is multifold. On one hand: our businesses/companies are underdeveloped when it comes to integration of digital technology dimension, and that automatically exposes them to higher cyber risks. The adoption of digital technologies by SMEs remains notably below the EU average (35% in the WB region compared to the EU average of 55%). On average, only 7% of WB enterprises used big data, 16% cloud and 3% artificial intelligence in 2021 [compared to 14%, 34% and 8% in the EU, respectively].

Governments of the WB should rapidly develop programmes and strategies that support digitalisation of business, including e-commerce. On the other hand, governments, technology companies, and businesses must join forces to develop and implement best practices, share threat intelligence, and create mechanisms for rapid response and recovery.

Dear all,

While preparing for this conference, we considered it particularly fitting to have a conference on resilient cybersecurity in WB here in Brussels - in the heart of EU and jointly organised with EC.

Fitting as our region’s cybersecurity is an intrinsic and inseparable part of Europe’s collective cybersecurity ecosystem. Acting together for stronger regional and EU cyber-capabilities and resilience are two sides of the same coin. The coin of international security and stability in cyberspace.

Also fitting as our region’s call for systemic integration of our region in EU’s overall cybersecurity efforts by design and by default – resonates loudest from here.

This call for much more structured cooperation and synergies relates to the full spectrum of: strategy, aligning policies, policy guidance, operational cooperation, preparedness, response and crisis management, investments, skills and awareness.

From being part of the policy dialogue, partaking in sectoral Council configurations, working groups, relevant agencies - to boosting access to knowledge, networks and also funds. As our policies can be aligned - but with the drastically different access to support instruments – the convergence gap in this area gallops.

RegionalCooperationCouncil

Co-funded by the European Union

That is why such regional high-level policy dialogue as this one we at RCC have to honour to convene - are so important. During these two days an impressive array of stakeholders, decision makers, partners and cyber talents discussed various facets of cyber resilience. What made these two days particular was strong and active contribution from committed EU MS and Commission services, hand-in-hand with our region's top presence.

In an environment with ever increasing number of connected objects in which our physical and digital infrastructures are very closely intertwined and in which cybersecurity threats are almost always cross-border – our region must be part of the "whole".

- Enhancing cyber resilience in the WB region remains a fundamental building block and backbone for all transformative changes. It will also be a fundamental building block for the new Growth Plan as any accelerated integration on e-commerce and the single market – presupposes resilient and safe digital environment.
- WB needs "plug-ins" in all EU bodies, networks, frameworks – in any capacity feasible. For quite some time, RCC is pushing to enable integration of the Western Balkans in the work of the European Union Agency for Cybersecurity (ENISA). This will mark another application of "phasing in" and contribute to an accelerated alignment of WB with the EU Single Market standards and practices.

Additionally, inclusion of Western Balkans in EU Cybersecurity Incident Review Mechanism to assess and review specific cybersecurity incidents would enable an enhanced response to cyber-attacks in the Western Balkans and build capacities for timely response.

Last,

If it would be measured as a country, cybercrime, which is predicted to inflict damages totalling 8 trillion USD globally in 2023, would be the third largest economy after US and China.

If studies and forecasts are scientifically right, an increase of 15% of cybercrime costs per year over the next 3 years will be the greatest transfer of economic wealth in history.

It means that the imperative to protect ourselves should be timeboxing.