GLOBSEC side event on Cyber Readiness of the CEE Region

by Francesca Spidalieri
Senior Fellow for Cyber Leadership at the Pell Center for International Relations and Public Policy at Salve Regina University &
CRI 2.0 co-author, Italy

- The **Cyber Readiness Index 2.0** is a comprehensive, comparative, experienced-based methodology to evaluate and measure a country's preparedness levels for certain cybersecurity risks.
  - 70 unique indicators across 7 essential elements to discern operationally ready activities and identify areas for improvement by leveraging or updating laws, policies, standards, market levers, etc.
- The CRI 2.0 demonstrates how national security is closely intertwined with Internet connectivity and rapid adoption of ICTs which, when secure, can lead to economic growth and prosperity. If the 7 essential elements are pursued in tandem, a country can better chart a path toward cyber readiness to defend against the economic erosion caused by cyber *insecurity* and protect their digital investments and the value of their economy.
- While **no country is cyber ready**, and few have aligned their digital agenda with their cybersecurity agenda, there are countries that have developed effective mechanisms to achieve cyber readiness/preparedness → bring attention to a country's most critical digital dependencies (e.g., companies, services, infrastructures, and assets) that, if harmed, would have grave economic and national security consequences.
- The economic opportunity of the Internet is at risk – we've embedded flawed technology and products in the core of our economy, critical infrastructure, & governments.
  - Legacy infrastructures + known vulnerabilities + flawed products & technology

- **Slovakia** is still in the early stages of developing the national capabilities needed to defend and respond to serious cyber threats (unclear what the consequences would be if a critical digital dependency were to be knocked offline).
- One of the top 5 most vulnerable countries in Europe to cybercrime + still highly depended on EU money to fund R&D projects, education & training programs.
- The Slovak government has launched important political and economic reforms since 1998 to accelerate Slovakia's development, connectivity, and digital economic growth. It also started to focus more on cybersecurity and cyber defense to be in line with EU and NATO requirements and calls to action.
- Since 2015, it has **decentralized** and **de-accelerated** some of these efforts, when responsibilities for the digital economy and cybersecurity of the country transitioned from the Ministry of Finance to NBU, DPM, and the Military Intelligence.
- The main challenge is that these two sets of goals – digital growth & national cybersecurity – are being executed by 3 separate entities today:
  - Digitization of the country & digital economic priorities led by the DPM Office;
  - Cyber resilience and cyber defense priorities (in time of peace) led by NBU;
  - Cyber defense in time of war or "serious event" by the Military Intelligence.
- Need to reconcile the economic and national security agendas → better align the digitization initiatives & digital investment strategies with the cybersecurity and cyber defense priorities → securing the digital economy must become a strategic priority!
- Establish clear lines of accountability & responsibility to ensure the execution of the country's objectives and implementation of risk reduction measures.

- Focus on outcomes (vs. policies) and whole-of-government approach.

<u>Strategic Considerations:</u>

Tie cybersecurity priorities to the 3 regional security and economic development initiatives (different goals & objectives) → there would be a natural synergy if they aligned their economic and security needs + wrap 12 countries under one umbrella:

- **Digital Three Seas Initiative**: a forum of 12 states in Central and Eastern Europe (Austria, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, Slovakia, and Slovenia) aimed at boosting digital economic development, increasing interconnectivity in the fields of energy, transport and digitalization, and improving infrastructure connections.

- **Bucharest Nine**: a platform of 9 states in Central and Easter Europe (Bulgaria, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, and Slovakia) aimed at strengthening the commitment of these states to the NATO, sharing views on a wide range of challenges and threats to the Euro-Atlantic area, and finding common responses to current security issues, especially the defense of the Eastern flank.

- **Visegrád Group**: a cultural and political alliance of 4 Central European states (Czech Republic, Hungary, Poland, and Slovakia).

1. It will be important that an audit/assessment be conducted on what are the baseline assets/infrastructures that are already in place in each of the 12 countries. The evaluation should be along at least three criteria: resilient; redundant; efficient. Focus on the North/South corridors too.
2. Consensus is needed among the Capitals on the future of the infrastructure build-out (e.g., 5G). It will be important to (1) harmonize the technological purchasing/use; (2) develop a common policy framework; (3) appreciate the total cost of ownership and not be seduced by 0% interest loans and low-cost products (i.e., China/Huawei and the digital belt-road initiative).
3. Develop a stronger narrative on the value proposition to invest in the 3 Seas Region - and specifically in the North/South Corridor. Define the quick-wins for investment (where is biggest bang for buck?)
   - Commercial: corporate investments will lead to a return on investment and drive the digital economy/digital growth
   - Government: be strategic. Do not enter into deals that might divide the Alliance (EU, NATO, etc).
4. Remember that there is a lot of technical talent in the region — the Soviets drew their talent from your technical universities. The 3 Seas Region, particularly Poland, Czech Republic, and Slovak Republic, have STEM universities.
   - Take an inventory of capacity in the region (current workforce development and university programs);
   - Incubate more talent (via Universities and corporate investment);
   - Retain the technical talent in the region as the region receives/attracts foreign direct investment and incubates new programs to support the 3 Seas Initiative.