IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

Hanns Seidel Stiftung
Ured u Zagrebu

02
2019

Towards the future in the Three Seas Region

By Izabela Albrycht

Introduction

Launched in 2016, the Three Seas Initiative (3SI) is designed to build cooperation and interconnectivity between 12 CEE countries through new cross-border infrastructures. The aim of the region's political leaders is to leverage the economic growth to the extent in which it can contribute to the EU's greater prosperity and at the same time tighten transatlantic bonds. Let us wish the 3S region yet another good year in which the 3S countries will see the materialisation of hopes", stated Kolinda Grabar-Kitarović, President of the Republic of Croatia at the Third 3SI Summit in 2018. She added: "substantial projects, such as energy supply corridors and communications infrastructure, as well as modernization of our economies through an extension of transportation links, will allow for the full integration of Central Europe with the remainder of our continent. It will annul the artificial, but still lingering division between old and new, West and East Europe and it will most definitely contribute to a higher level of prosperity of Europe as a whole."

The way forward

While advancing 3S cooperation, the decision makers need to bear in mind that the future will all be relied on cyberspace that is already dramatically changing the rules of the game. With cyberspace being another determinant of geostrategic and geoeconomic potential of states, it has given rise to a new arena of competition, innovation and security. ”I believe in the Initiative's potential, as it builds on the real need of the 12 participating states to reach the real convergence of their economies with the Western part of the EU,” said Klaus Iohannis, President of Romania. Moreover, the digital transformation of the region is in fact the way to turn this belief into a reality. That is why the 3S cooperation should also be aimed at encouraging the states to climb up the global supply chain ladder in IT and cybersecurity sectors, boosting cross-border industrial scientific research and development cooperation, and attracting international and domestic investments in the region.

> *While advancing 3S cooperation, the decision makers need to bear in mind that the future will all be relied on cyberspace.*

However, on the operational level, over the last two years, most of the 3S planned projects have mainly focused on breaching big infrastructural gaps in transport and energy sectors which, in fact, had undermined the economic growth of the region for decades, but in years to come, will not be the only two problems hindering regional cohesion. In the era of “technology of everything” and everything being smart thanks to a connection to the internet, it is the digital realm which should now be a centre of gravity when it comes to political and economic consideration within the region. There are more than a few important reasons for that.

> *Development and implementation of new hi-tech solutions and deployment of the next generation digital infrastructures are prerequisites for the future economic growth.*

First, the development and implementation of new hi-tech solutions into the public and the private sector, as well as a rapid deployment of the next generation digital infrastructures, are prerequisites for the future economic growth. Second, physical infrastructure connecting the region will implement ICT elements and will be plugged to the Internet, which will pose an existential threat if not be properly secured. If there is no focus on cybersecurity issues in the region, this infrastructure gap that we are now trying to address will not be the only problematic one because it will be followed by a security gap. In other words, adding cybersecurity dimension across three pillars of cooperation and deploying infrastructure in "security by design" mode as well as strengthening of the third digital pillar is the only way to make the 3SI architects' dreams come true.

> *Adding cybersecurity dimension across three pillars of cooperation and deploying infrastructure in "security by design" mode is the only way to make the 3SI architects' dreams come true.*

An increased focus on digital issues can boost the initiative itself. The dynamics of integration is relatively slow and we can also observe certain tensions within the 3SI countries related especially to energy issues. However, when it comes to digital challenges, all 3SI countries have collaborated successfully on the EU arena.

Considering all of those factors, in June 2018, a group of regional think tanks launched the Digital 3SI that emphasizes the importance of the digital pillar and the need to establish a horizontal cybersecurity dimension. The Digital 3SI consists of several project and joint-action proposals aimed at building digital cooperation, including cybersecurity cooperation, as well as digital infrastructure deployment, regional support in digital transformation and education of digitally skilled societies.

Cybersecurity cooperation and investments

Cybersecurity cooperation among the 3S countries should go horizontally across the following three pillars: energy, transport, and digital, in order to strengthen the resilience of national and regional infrastructures. Being heavily exposed to cyberattacks and cyber disruptions, the 3S region should also focus more on advancing its cyber capacity building. It can be done within the framework of EU policies and strategies, such as the newly presented Cybersecurity Act, and within the international context, especially in collaboration with the U.S. A stronger American international engagement was introduced in the U.S. National Cyber Strategy called the Cyber Deterrence Initiative. Given its cybersecurity exposition to hostile state activity, CEE should actively advocate for partnering in this initiative as it is now being carefully designed. The U.S.-3S cooperation can be based on government-to-government best practice sharing, strengthening cyber resilience and deterrence posture by pooling resources, sharing information and intelligence and building advanced capabilities. Nevertheless, it could also be concentrated on deployment of innovative technologies thanks to technology transfer due to an increase of foreign direct investments in the region by the U.S. companies. These developments would positively resonate with both the 3S region and the EU, enhancing their economies and strengthening their cybersecurity postures. Domestic companies should also ramp up their investments in the cybersecurity sector and together with universities team up in talent education, as they are major engines of growth that can be supplemented with a fairly intense trade between the countries of the region. The potential of the cybersecurity market in the 3S is rapidly growing thanks to the population size, demographic trends, the number and turnover of companies, as well as the pace of economic growth. Furthermore, it happens also due to changing labour costs and the current level of 3S trade exchange, as well as because of the massive expand of cyberattacks surface and the regulatory regime.

> *Domestic companies should also ramp up their investments in the cybersecurity sector and together with universities team up in talent education.*

According to a report "a significant share of import of cyber security solutions - in 2016 in nine CEE countries, imports amounted to almost EUR 2.2 billion (about 20 % of total EU imports), which means high demand for products and services that cannot be offered by domestic companies. In addition, most of this import came from countries outside the EU". In 2017, there were over 111 million consumers in the 3S region, which accounts for 21.76 % of the total EU population. It is predicted that the intensity of digital and cybersecurity technology usage will concentrate within three main groups of customers: individuals, entrepreneurs and the public sector. The development of the IT security market in the EU is shaped by regulatory factors, such as new legislation in the area of cybersecurity, and the market factors related to a wide spread of digital technologies in everyday business and social life, which is accompanied by increased security threats.

Digital infrastructure and security of 5G

The realisation of this grand idea should start with the 3 Seas Digital Highway (3SDH) that will underpin the future economy and is likely the low-hanging fruit among all the 3S projects we are all looking ahead to in 2019. Deployment of joint cross-border digital infrastructure projects, with the 3 Seas Digital Highway as a flagship initiative, will enable better and more secure data transfer along the north-south axis of the region, bridging the gaps in the communication infrastructure. The 3SDH should consists of fibre optics (both backbone and access layers) and 5G technology infrastructure, both complementing transport infrastructures built as part of the 3SI projects, such as Via Carpatia.

The Digital Highway should serve as a backbone of the data economy in the region together with data-driven industries. Modern cloud-based services and data centres (the so-called 3S data islands) should be built along the Highway, enhancing the implementation of emerging technologies like autonomous vehicle, AI, IoT as well as the development of e-commerce centres, such as DIHs and Competence Centres across the region. On 17 September 2018, the leaders of the 3S countries who had gathered in Bucharest for the third 3S Summit shortlisted main strategic projects in energy, transport and digital domains which also included the 3 Seas Digital Highway project developed in partnership with the Ministry of Digital Affairs in Poland.

> *The realisation of this grand idea should start with the 3 Seas Digital Highway that consists of fibre optics and 5G technology infrastructure.*

It is worth emphasising that the deployment of the 3SDH should be preceded by cybersecurity considerations about common security models and standards for 5G networks. It is critically important since the debate about the security of digital value chains as well as technology provenance with 5G being a key enabler of the future digital world is now rapidly advancing and gaining attention of the EU, NATO and particularly U.S. decision-makers.

Emerging new digital technologies

New breakthrough technologies are posing integration challenges that hinder digital transformation of the 3S region that is already lagging behind the world and the Western Europe. It is due to the speed with which its economies are digitally transforming but also with regard to digital innovativeness rates. In 2017, the share of the 3S countries in the total GDP of the EU equalled 10.81 % whereas the GDP per capita was lower than the EU average in all 3S countries except Austria. The average GDP growth rate was 4.2 %, exceeding the EU average of 2.4 % by 1.8 percentage points. Secure digital transformation can foster the process of reducing economic disparities. Countries of the 3S region should therefore pool resources together to overcome strategic and operational challenges of cloud computing integration within the public and the private sector, AI development in terms of easier access to data and deployment of secure 5G infrastructure. Additionally, collaboration between the region's most innovative entities such as universities, R&D centres, Digital Innovation Hubs and Competence Centres will facilitate the creation of a successful and innovation-friendly ecosystem.

Joint technology initiatives can speed up the development of Industry 4.0 by promoting matured high technologies based on the industry's needs, including autonomous transport, electromobility, FinTech, HealthTech, smart solutions for cities, and the exchange of know-how that advances the digital transformation of CEE.

Digital education

It needs to be highlighted that only by educating the 3S digitally savvy societies we can unlock the bright future for the 3S region. This, in turn, will boost the growth of the ICT sector and transform the region's countries into more innovative data-based economies. Digital future depends on sufficient amount of ICT talent, therefore special emphasis should be placed on the so-called STEM (which stands for Science, Technology, Engineering and Mathematics) in education. 3S region countries are not systemically prepared to face cyber threats and challenges, and their education systems have not kept pace with the market needs. This state of affairs threatens the internal, international and economic security. 3S decision-makers need to be aware of these threats and need to increase expenditures on education and adjust educational offerings, as well as introduce solutions to the challenge of brain drain. It is essential to support the academic centres that serve as recruitment base for the broader cybersecurity and digital sector. Additionally, according to the newly released report, in order to achieve this, we should also continue building the capacity of ICT trainers through a variety of means including:

- the establishment of adequate budgets for teacher training and identification of skills required by the industry,
- the support for the development of new technologies' departments at universities by cooperating with the private sector,
- the establishment of national training schemes to address the mismatch of skills as well as industry-sponsored MSc and PhD programmes and STEM platforms as part of the EU STEM coalition,
- the increase of the government-industry cooperation,
- the establishment of equality benchmarks to reduce inequality in computer science education and eliminate gender bias.

The 3SI is in 2019 of special importance to the U.S. as the country is now striving to counter the expansion of China's Belt and Road Initiative and the so-called "Digital Silk Road" with emerging technologies on its disposal such as 5G or AI. In the geopolitical sense, the 3SI is in fact yet another scene to reiterate the memorable phrase "united we stand, divided we fall." The initiative, as it was described by one of its architects, prof. Krzysztof Szczerski, Chief of Cabinet of the President of Poland, at the Heritage Foundation in March 2018, is also "a project of the future".

Izabela Albrycht is the Chairperson at the Kosciuszko Institute in Krakow, Poland.

DISCLAIMER: The views presented in this paper are solely of the author and do not represent an official position of the Institute for Development and International Relations or of the Hanns Seidel Foundation.

IRMO
Institut za razvoj i međunarodne odnose
Institute for Development and International Relations

Hanns
Seidel
Stiftung
Ured u Zagrebu

Institute for Development and International
Relations - IRMO
Lj. F. Vukotinovića 2, Zagreb, Croatia
www. irmo.hr

Hanns Seidel Stiftung
Amruševa 9, Zagreb, Croatia
www. hanns-seidel-stiftung.com.hr