June 2018

THE KOSCIUSZKO INSTITUTE POLICY BRIEF

THE DIGITAL 3 SEAS INITIATIVE: A CALL FOR A CYBER UPGRADE OF REGIONAL COOPERATION

WHITE PAPER

EXECUTIVE SUMMARY

With the advent of cyberspace, the rules of the game have changed irrevocably. A new arena has emerged where geography no longer restricts individual players. Cyberspace has become another determinant of geostrategic and geoeconomic potential of states.

The authors of the following White Paper call for a range of activities aimed at building digital cooperation in Central and Eastern Europe under the name of the Digital 3 Seas Initiative which would include:

1) **Development of the digital pillar within the Three Seas Initiative should be rapidly enhanced and cybersecurity needs to be included in three pillars: energy, transport, digital.**

2) **Joint cross-border infrastructure projects** (e.g. the 3 Seas Digital Highway) that enable better and more secure data transfer from north to south of the region and bridge the gaps in the communication infrastructure, including fibre optics, 5G technology infrastructure, data islands, complementing energy and transport infrastructures built as part of the Three Seas Initiative projects;

3) Joint initiatives to tackle **integration challenges with new technologies and solutions** that significantly hinder digital transformation of the Three Seas region (e.g. strategic and operational challenges of **cloud computing** integration within the public and the private sector);

4) Development of **common security models and standards for 5G** networks based on the security by design principle;

5) Elaboration on and implementation of the **free flow of non-personal data policy** which underpins innovative and data-driven industry and breakthrough technologies (e.g. Artificial Intelligence, the Internet of Things);

6) **Joint technology initiatives** to strengthen cross-border industrial scientific research and educational cooperation (e.g. autonomous transport, electromobility infrastructure, smart solutions for cities, blockchain) to advance the digital transformation of CEE and the exchange of knowledge;

7) Fostering the **development of Industry 4.0** (e.g. FinTech, cybersecurity, electromobility, HealthTech), which already gives CEE comparative advantage in the global market;

ISSN 1689-9873

8) Strengthening and securing **e-commerce centres** in locations strategic for the whole region through the construction of smart storage systems and smart customs clearance;

9) Security cooperation on **countering information warfare** based on the common experience and high exposure to hybrid threats within the region;

10) Boosting collaboration, integration and trust among **Digital Innovation Hubs, Competence Centres** and global and regional companies (e.g. developing partnerships and platforms, enhancing the dissemination of digital innovation, promoting matured technologies based on the industry's needs);

11) Boosting the region's involvement in the **development of cybersecurity policies** and strategic concepts at the European level.

Introduction to the concept

Mountains, seas and rivers, which make Europe so enchanting, led to the emergence of an equally diverse political and economic landscape. Geography has always been a decisive factor in determining the economic potential of countries, the location of industrial centres, the shape of alliances, or the delimitation of borders. This is particularly evident in Central and Eastern Europe.

The approach to cyberspace taken by the countries in the region will shape the 21st-century Europe's digital map. Therefore, we can either reproduce the old dividing lines, following geographic boundaries, or build infrastructure that will deepen cooperation. Joint cross-border infrastructural projects, advancements in digital transformation and effective cooperation models within and across countries and sectors will determine the future of Europe. We can draw a digital map that will either consist of modern European states interconnected with digital rivers and the free flow of data, or a collection of alienated states, isolating themselves within their political borders. The success of this process is important not only for the countries of the region, but also for the cohesion of the EU and the transatlantic community.

What is the Digital 3 Seas Initiative?

The Digital 3 Seas is a portfolio of cross-border projects and initiatives that aim to develop digital infrastructure, joint investments and R&D, as well as political and legislative concepts implemented at the EU level. The central idea is the incorporation of the ***security by design*** concept into the digital transition of the public and the private sector. The Digital 3 Seas builds upon transport and energy infrastructure networks that constitute the backbone of the Three Seas Initiative and supplements it with a cyber dimension.

What is the Three Seas Initiative?

The Three Seas (also known as the Three Seas Initiative, 3SI) is a political and economic project inaugurated in 2016 that aims to deepen the integration of the countries of Central and Eastern Europe and strengthen their position in the European Union.

Why does it matter?

The Three Seas comprises 12 EU countries and 114 million of citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion.

The ever-changing global security architecture renders the region increasingly vital for actors as varied as the U.S., Great Britain, China or Russia. Upgrading the Three Seas Initiative by strengthening the digital component, that exists next to transportation and energy components and adding cybersecurity dimension may have geopolitical and geoeconomic consequences far beyond the CEE borders.

The Three Seas is especially important to the U.S. as it will strive to contain the influence of China's Belt and Road Initiative (with the so-called 'Digital Silk Road'). Through the 16+1 format, China seeks to pursue the realisation of the European part of the Belt and Road Initiative and the geographic location of CEE is crucial for building connectivity between Europe and the Far East.

The Digital 3 Seas has great potential to build synergy with such projects as the Digital Single Market, under normative limits and the framework set by the EU.

MAPPING THE DIGITAL 3 SEAS – SECURE DIGITAL INFRASTRUCTURE AND SMART POLICIES

- **The 3 Seas Digital Highway** envisages building a fibre-optic and 5G infrastructure along the already planned transport and energy routes;
- Hubs for services based on **cloud computing** and **data storage** – the so-called **data islands** – could sprout along the **3 Seas Digital Highway**;
- **The free flow of data** would eliminate the necessity to duplicate infrastructure for digital resources storage, thus connecting the **data islands** across the region and enabling the data-driven economy;
- Enhanced secure telecommunications infrastructure together with intelligent storage systems and smart customs clearance could facilitate the creation of **e-commerce centres** near transportation hubs.

IMPLEMENTING THE DIGITAL 3 SEAS INITIATIVE – THE ACTION PLAN FOR 2018:

- **Engaging think tanks and experts** from the region, the U.S. and the United Kingdom;
- Launching the **Digital 3 Seas Business Forum;**
- Crafting a detailed **strategy for implementation** of the digital component into the Three Seas Initiative;
- Promoting the Initiative at **CYBERSEC 2018 in Kraków** (8-9 October 2018);
- Advocating for the digital component to be officially included in the Three Seas Initiative at **The Three Seas Summit in Romania** (Autumn 2018).

THE THREE SEAS INITIATIVE

The Three Seas Initiative (3SI) is a political and economic inter-governmental project aimed at deepening the integration of the countries of Central and Eastern Europe (CEE) and strengthening their position in the European Union (EU). Inaugurated in August 2016 by the President of Poland, Andrzej Duda, and the President of Croatia, Kolinda Grabar-Kitarovic, the initiative is designed to encourage multifaceted collaboration, especially in the area of economics and infrastructure. The Three Seas Initiative comprises 12 EU countries and 22 percent of EU citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion.

Both the Three Seas Initiative and the Bucharest Nine (B9), a cooperation project of the nations on NATO's eastern flank which works on similar principles and have a comparable territorial coverage to the Three Seas Initiative, prove a growing need for establishing a strong regional cooperation framework within the EU.

Dynamic digital transformation of CEE economies, an ever-increasing significance of cyberspace in international relations, and new borderless hybrid security threats call for the Three Seas Initiative to be given a strong digital dimension, with a cybersecurity component as its indispensable element.

The threats in the CEE region and the rest of Europe share to some extent a common denominator; however, the CEE region is also a testing ground for some threat campaigns, which can then further resonate geographically. CEE countries, just as any other region in the world, are threatened by various forms of cyberattacks. However, what puts the nations at a particular risk is their greater exposure to conventional conflicts that are increasingly being accompanied by sinister activities in cyberspace, which stems from their location in a geopolitically tense region. The CEE countries that are NATO members strongly advocate for strengthening NATO's presence in the region, seeing it as the guarantor of their safety. A conventional, open military conflict is an unlikely scenario as any decision to launch a large-scale military attack would be extremely risky from the aggressor's point of view.

However, CEE countries are highly exposed to a wide range of cyber operations, not only those that include cyberattacks on information technology (IT) or operational technology (OT) systems, but also those seeking to manipulate people's perception. The reason for that is that CEE countries are involved in strategic, often tense relations with actors who understand and apply cyber operations in a very broad way. History has shown that many cyberattacks, especially those aiming to breach national security, were first carried out in the CEE region (e.g. a large-scale cyberattack on Estonia, disinformation campaigns in Poland, etc.).

The Digital 3 Seas Initiative has potential to foster joint cross-border technological projects, political and legislative concepts at the EU level, as well as scientific and educational cooperation and the development of secure digital infrastructure. Strong regional cooperation is also essential to accelerate the pace and nature of global digital changes. Joining the group of cyber superpowers requires smaller countries to pull resources within a well-structured cooperation framework.

The Digital 3 Seas Initiative should be perceived as such framework and as a complementary project, fitting in with the existing EU schemes, such as the Digital Single Market and the Connecting Europe Facility. The project members should cooperate closely with their partners from the EU and NATO. The Initiative should also be viewed as a unique source of knowledge for Allies because what happens to that region in cyberspace today, is very likely to happen to their homelands tomorrow.

The Three Seas Initiative is 'the concept' for CEE and is strategically supported by the U.S.

"The Three Seas Initiative will not only empower your people to prosper, but it will ensure that your nations remain sovereign, secure, and free from foreign coercion. The Three Seas nations will stand stronger than they have stood before. When your nations are strong, all the free nations of Europe are stronger, and the West becomes stronger as well."
U.S. President Donald Trump in a speech given to the Three Seas countries' leaders at the Three Seas Summit in Warsaw on 6 July 2017

"An important component in the U.S. strategy is to encourage closer political and economic cooperation at the regional level, among the Allies most vulnerable to supply manipulation in Central and Eastern Europe. Lack of seriousness about the need to increase North-South infrastructure in the space between the Baltic and Black Seas has been a contributing factor to Europe's geopolitical vulnerability in the East. We have prioritized U.S. engagement in regional groupings such as the Three Seas Initiative, Visegrad Group, Bucharest Nine, and Nordic-Baltic group as platforms for bolstering the region's resilience against energy coercion."
A. Wess Mitchell, Assistant Secretary of State for European and Eurasian Affairs, Senate Foreign Relations Committee, Subcommittee on Europe and Regional Security Cooperation, 12 December 2017

THE THREE SEAS INITIATIVE AND ITS INTERNATIONAL CONTEXT

Recent years have brought noticeable changes on the geopolitical chessboard. The EU is changing its face before our very eyes. In highly uncertain times marked by the EU's feeble economic growth, immigration crisis and increasing centrifugal trends which culminated in the Brexit vote, new momentum is needed to prevent further decomposition of the EU. The EU countries must build concepts that will reintegrate them around new projects and enterprises. They should focus on pursuing common interests of individual states, building their political and economic advantage, but at the same time contribute to achieving the goals of the EU policies. As there is no strong EU without strong CEE, in the rapidly changing reality, the Three Seas Initiative with a digital component has every chance of adding value to European integration.

While the post-Brexit UK will seek to establish bilateral relations with EU Member States, embracing closer cooperation with the Three Seas nations seems a natural direction to pursue. On the other hand, cooperation between the U.S. and CEE countries may constitute an essential link enabling the U.S. to maintain their strategic presence in Europe and therefore guarantee that the idea of transatlantic integrity is further pursued.

CEE is becoming a critical region in the geopolitical power struggle between China and the U.S. Beijing's grand geopolitical project – the Belt and Road Initiative – sees CEE as a 'gateway into Europe'. China recognises the significance of this region, trying to strengthen its political and economic influence in this part of Europe. The main platform for this activity is the CEEC Forum, also known as the '16+1'. Inaugurated in 2012, the project comprises 16 countries from the CEE region, including 11 EU member states.

One cannot forget that CEE, being adjacent to Russia, is an external eastern frontier of the EU and NATO. In light of Moscow's aggressive policy in both conventional and digital dimensions (armed conflict in Ukraine, expeditionary operations in Syria, resumption of strategic bomber and nuclear submarine patrols, the strengthening and modernisation of the so-called nuclear triad, large-scale military exercises with the use of large groups of airborne troops and aviation strategic units, military doctrine declaring that Russia remains in a state of permanent conflict, influencing the course of election campaigns

in the U.S. and France, sponsoring and inspiring cyberattacks, cyber espionage, more or less explicit development of offensive capacities to conduct military operations in cyberspace, using cyber tools for hybrid operations), this has enormous strategic and economic implications.

For all these reasons, CEE is a pivotal area on the 21st-century geopolitical map. Due to joint projects carried out within the Digital 3 Seas Initiative framework, the region can gain yet another comparative advantage and become a driving force for the EU economic growth and a critical component of the new global security architecture.

CEE is a pivotal area on the 21st-century geopolitical map.

THE 3 SEAS DIGITAL HIGHWAY

The current Three Seas Initiative stipulates predominantly the expansion of energy and transport infrastructures, aiming to connect north and south of the region. However, the concept should be further expanded to include a secure data transmission element. The Three Seas should be linked via the so-called *3 Seas Digital Highway*. In 2015, the Baltic Highway, a fibre-optic network connecting Tallinn and Frankfurt via Riga, Vilnius, Warsaw and Berlin, was officially launched. Like many other similar investment projects, it aims to connect Western and Eastern Europe. The Three Seas Initiative, connecting the Baltic Sea, the Adriatic Sea and the Black Sea, should also consider, as its integral part, the development of secure digital infrastructure along the north-south axis. This will help complement the map of digital connections that are currently the foundation underpinning digitally evolving economies. The concept of supplementing gas and road infrastructures being built as part of the Three Seas Initiative with a secure digital component should be further elaborated and extended to all the countries participating in the Initiative. The synergy may additionally shorten the time required for the investment process and lower the cost of the enterprise.

The construction of the 3 Seas Digital Highway can help develop modern 5G wireless technology and the whole ecosystem that is founded on it and common for all CEE countries. As a platform to connect to different radio technologies in a flexible way, it is expected that the fifth-generation mobile system, with technical parameters suited to provide endpoint services, will revolutionise mobile telecommunications and provide access to new mobile technologies not only to citizens, but also, on a large scale, to companies, especially those fitting in the 'Industry 4.0' concept, that will build upon it their competitive advantage. Poland is one of the countries in the region that invest in the expansion of mobile networks, providing for the subsequent versions of the standards, and thus in the concept of a 'mobile state' and the data-driven economy – 'Industry +'. Access to high-speed Internet underpins economic development and e-society founded on the principle of the digital market (free movement of data, e-commerce, etc.) today by 4G mobile network base stations (LTE and LTE-Advanced), and in the future by 5G networks, linked mainly to fibre-optic networks. High-speed Internet connections also enable a better integrated crisis management and reporting system. A fibre-optic network, both skeleton and access network, supplemented with 5G technology could breach the gaps in the communications infrastructure between CEE and EU-15. This would further deepen digital cooperation throughout Europe, contributing significantly to the competitiveness of the region and meeting the objectives of the Digital Single Market. In addition, the skeleton of this international fibre-optic network would allow for the exchange of growing roaming traffic, either at the level of the Internet access itself or 5G network specialised services; for example, it would enable a vertical exchange of data between factories located in different countries and operating in accordance with the "Industry 4.0" concept.

In order to build the 3 Seas Digital Highway, it is necessary to ensure data security. Fibre-optic cables are not only located underground or on the surface, but also lie in the oceans and run along seabed. Although it is difficult to tap these cables, it is possible to do so at junction points. Successful attacks on fibre-optic cables can cause the country to be deprived of global Internet access. Ensuring resilience of the undersea and terrestrial fibre-optic infrastructure to damage and new threats requires encryption and supervision

through appropriate systems and procedures. Due to the key role of the region as NATO's eastern flank and in view of the increasing activity of Russian unmanned underwater vehicles in the close vicinity of undersea fibre-optic cables, the issue needs to be placed high on the political agenda of the Digital 3 Seas Initiative.

On the other hand, in order to build the confidence of citizens and industry in 5G technology, it is necessary to take into account the cybersecurity component in the entire multi-layered fifth generation network architecture, which, in addition to high technical parameters, should be primarily characterised by reliability and integrity. Hence, it is important to 'approach 5G security in a comprehensive manner, not only at the level of network services, but also in the higher layers related to the provision of specific services.'[1] To meet this condition, it is appropriate to develop criteria for the selection of subcontractors, including telecommunications service operators, cloud-based service providers, vertical and virtual private 5G networks. The discussion on the topic has already commenced in the U.S. which is considering the exclusion of certain companies from the participation in the investment process for security reasons. The U.S. wishes to work closely with its allies in this respect. It can therefore be assumed that the development of common security models and good practices related to the construction of 5G networks may take place not only on the designated international forums, but also as part of the Digital 3 Seas initiative as the technology is now taking off around the globe

Imagine Central and Eastern Europe in 2030...

Imagine a fleet of electric, autonomous vehicles driving themselves through Krakow – until recently one of the most polluted and congested cities in Europe. When the first autonomous cars for the residents appeared on the city streets in 2025, no one ever imagined that the technology would be able to improve the quality of life in the city in such a short period of time. However, the project launched by the local government in 2020, had every chance to succeed. At that stage, the city had already been a thriving living lab for smart city secure solutions with a dynamically implemented 5G infrastructure. The usage of modern data centres in the Czech Republic and Slovakia had been factored in as early as the project phase. Access to them had been made possible by cross-border high-bandwidth fibre-optic connections, which had started to cover the CEE territory along with the development of 5G infrastructure. This was pivotal to the success of the project, which would have otherwise been unprofitable if based solely on services provided by external partners. The project would have also been impossible if it had not been for the free flow of data, which greatly simplified the work on large amounts of data in a project as ambitious as the fleet of autonomous vehicles.

THE ECONOMIC DIMENSION OF THE DIGITAL 3 SEAS INITIATIVE

The construction of a modern, robust and secure technology infrastructure can be an incentive for strategic domestic and foreign investment, promote development and strengthen the position of the companies operating in the region. They will benefit from the possibility to increase their market share in the countries which are parties to the agreement; in addition, due to an easier exchange of information and know-how, they will experience the 'spill-over' technological effect, involving the transfer of knowledge and skills in areas where a technology gap persists.

The so-called data islands, i.e. hubs for services based on safe and secure cloud computing and data storage, should be created along the 3 Seas Digital Highway. This may spur public-private cooperation focused on building secure digital economy. These kinds of centres will contribute to creating new and strengthening the already existing Digital Innovation Hubs (DIH)[2] that aim to promote Industry

1 Polish Ministry of Digital Affairs, Strategia 5G dla Polski, p. 35

2 R. Siudak, Z. Jóźwik, Regional innovation centres and their role in dealing with cyber disruption, The Kosciuszko Institute, Kraków 2017, http://www.ik.org.pl/wp-content/uploads/policy-brief_regional-innovation-centres-and-their-role-in-dealing-with-cyber-disruption.pdf

4.0 by stimulating cooperation between research units, entrepreneurs and the public sector. The 3 Seas Digital Highway, along with a network of interconnected hubs, will accelerate the digital transformation of the economies in the region, thus strengthening the role of CEE within the EU's Industry 4.0 and Digital Innovation Hubs agendas. But it is also essential to start a discussion on how to tackle integration challenges with new technologies and solutions that significantly hinder digital transformation of the Three Seas region (e.g. strategic and operational challenges of cloud computing integration within the public and the private sector).

Enhanced telecommunications infrastructure will also enable the creation of e-commerce centres in locations strategic for the entire region to facilitate export business. One of such centres could be the Central Communication Port, a large transport hub project currently under way that is planned to be located in the geographic centre of Europe, between Warsaw and Łódź, or the transport hub located in Constanța – the largest maritime port at the Black Sea.[3] They will aim to integrate railway, road and air transport nodes. The establishment of a centre with such tremendous logistical advantages will constitute a perfect ecosystem for the advancement of e-commerce facilitation solutions, such as the development of intelligent storage systems and smart customs clearance. In order to help initiatives involving electronic services and digitalisation of logistics thrive successfully, it is necessary to lay solid cybersecurity foundations to ensure trust between entrepreneurs and suppliers of the above-mentioned services. Only transparent and reliable instruments will effectively contribute to streamlining commercial processes and, as a consequence, to boosting e-commerce growth.

The innovative ICT environment of e-commerce centres could facilitate the development of a number of solutions based on Artificial Intelligence and the Internet of Things which require a creative environment with high technology absorptive capacity, as well as a society aware of opportunities and threats. Therefore, it is anticipated that this environment will result in a dynamic expansion of autonomous transport, infrastructure suitable for electromobility and smart city (and countryside) solutions, such as smart grids, distributed energy, smart street lighting and road traffic systems, smart residential security systems, or even cornfield supervising systems. In view of a strong connection between the effectiveness and efficiency of these solutions and the transfer of real-time data, secure and modern back-end network systems are needed, for example 5G networks.

Europe's digital advancement is not possible without the cross-border free flow of data. It eliminates the necessity to store digital resources in multiple locations, which reduces the need for duplication of expenditure on IT systems, thus optimising the associated costs. The free flow of data is critical for the development of data-driven economy, for example by stimulating the creation of new products and services using resources such as open databases or *big data* sets. This issue is particularly important for making SMEs more competitive.

Recent years have been marked by a significant development of the startup stage in CEE. The digital economy revolution proved to be a great opportunity for innovation drawing upon solid technological and engineering foundations laid by academic centres of the region. The next key step should be to support the growth of selected sectors of the Industry 4.0, such as FinTech, cybersecurity, electromobility or HealthTech, which already helped CEE build comparative advantage in the global market. Due to economies of scale and the problem of internal markets in individual countries being insufficiently large, dedicated acceleration programmes should encompass the entire region, becoming a springboard for local and global expansion of startups participating in those projects.

The Digital 3 Seas Initiative may become a global forerunner in the responsible use of distributed ledger technologies such as *blockchain* which is both a transaction system and a data storage technology. Cryptographic mechanisms protect the stored information, which, as a rule, must not be changed or removed. These types of initiatives include the creation of one's own cryptocurrency,[4] supply chain management

3 Constanta is located at the junction of 3 Trans-European Transport and commercial corridors (Corridor IV, IX and VII Danube).

4 A wide range of countries, like Estonia, is currently considering such an option. See Kaspar Korjus, We're planning to launch estcoin—and that's only the start, https://medium.com/e-residency-blog/were-planning-to-launch-estcoin-and-that-s-only-the-start-310aba7f3790

in *blockchain*, the creation of distributed (and thus more secure) databases, smart contracts, or intellectual property protection systems. In addition, one of the advantages of the blockchain technology is the disintermediation – the ability to remove any intermediaries from the supply chain. This can help build services based on a direct relationship between CEE countries and their citizens within the Digital 3 Seas Initiative. An example of that could be a toll system using solely a smartphone application (created by the state), digital maps and a distributed ledger technology. The simplicity and innovativeness of the concept could help take the solution to the next level, which is the expansion to other EU countries.

Today, the potential of the blockchain technology is widely recognised by all sectors of the economy. Only during the first nine months of 2016, startups using the blockchain technology attracted investment worth USD 1.4 billion.[5]

It is important to note that the countries of the Three Seas Initiative should actively and collectively engage in the EU's High-Performance Computing (HPC) project.

All these initiatives will contribute to strengthening the already existing Digital Single Market by using digital economy processes as a stimulus for growth both in the region and across the EU.

Imagine Central and Eastern Europe in 2035...

Krakow's success showed that the technology of autonomous vehicles can transform a city in a revolutionary way. The project has been replicated in many cities of the region. An increased demand for big data processing services has made data islands in the Czech Republic and Slovakia grow into real giants that develop solutions adapted all over the world. International bus connections have been autonomised, also with the participation of Polish producers, who could have tapped into a real treasure trove of knowledge accumulated during autonomous vehicle pilot projects run across CEE. Clever implementation of 5G technology accompanying the expansion of road connections has enabled autonomous vehicles to travel from Tallinn to Zagreb without breaks in access to the network.

Without such a well-developed network, e-commerce hubs in CEE could not have reached such a high level of growth. With a fleet of driving and flying autonomous postal vehicles built in a joint effort among the 12 countries of the Digital Three Seas Initiative, the cost and shipping time of cross-country deliveries in the region does not differ from national deliveries. It is hard to overestimate the impact of this infrastructure on the boom in the segment of SMEs which has been observed in the region for the last several years.

Only a decade ago, cybersecurity was a domain that only the military as well as the financial and the IT sectors were concerned about. Today, the need for enhancing cybersecurity is growing also in other domains. The sabotage attack on the Ukrainian power grids in 2016 proved how significant and serious consequences such attacks can have for the critical infrastructure. A number of studies confirm that energy and communications/transport sectors are particularly exposed:

- According to the Ponemon Institute, cybercrime causes losses of USD 12.8 million annually in the energy sector and public utility services;
- PWC reports that the number of attacks in the energy sector grows six times each year;
- Over 1,000 serious cyberattacks are carried out monthly against the aviation industry;
- Cisco reports that in 2016, attacks on IoT grew up to 172 percent;
- Telefonica estimates that 90 percent of cars will be connected to the Internet till 2020;
- The U.S. Department of Homeland Security warns that attacks against the critical infrastructure are cheaper and safer (because of problems with attribution) to carry out, but can be dreadful in consequences.

All that the findings lead to a conclusion that cybersecurity should not only be present in one of the Three Seas pillars, namely the digital pillar, but also should be included in those of energy and transport.

5 https://exbino.com/exbino_artykuly/blockchain-startupy-przyciagnely-inwestycje-na-14-mld-usd/

CHINA IN CEE

Many countries of the Three Seas Initiative enjoy close links with China and share numerous declarations of willingness to participate in the Belt and Road Initiative, in which the digital dimension constitutes one of the elements. It is necessary to make a careful evaluation of the areas of cooperation to use business opportunities effectively and adequately protect the strategic interests of the countries of the Three Seas Initiative, NATO and the EU.

The document issued by the National Development and Reform Commission of the People's Republic of China (PRC) in 2015[6] enumerates the components of the so-called Information Silk Road: the construction of cross-border and submarine optical networks as well as the implementation of satellite communication projects. The above-mentioned technologies assume extensive dependence on the manufacturer who has control over the flow of information and access to its content. Insofar as Beijing's actions are limited mainly to declarations in the context of the 16+1 initiative, the countries with closer ties to China have already implemented pilot projects. Having signed a preferential agreement with China, Pakistan has received a modern BeiDou satellite navigation system to be used for military and civilian purposes, which is an alternative to the American GPS standard or the Russian GLONASS.[7] By the same token, China has gained a tool to exert political pressure on the contracting partner, which in light of Pakistan's nuclear potential takes on strategic significance. The combination of economic and political motivations, so characteristic of Beijing's international activities, is clearly present here.

It is necessary to carefully select the areas where China's involvement in the Digital 3 Seas projects will deliver win-win economic outcomes and not generate strategic security issues. One of such areas could be e-commerce at communications hubs. One of the steps toward seeing the idea materialise is the agreement signed in 2017 between the Polish Post and its counterpart, the China Post, for the road transport of postal matters to Europe, which involves establishing a dedicated logistics hub.

China implements the cooperation model offered in the 16+1 format all over the world, mainly in developing countries which tend to hit more stumbling blocks to obtain the funds for infrastructure projects than the EU members. Investments or loans offered as part of the 16+1 initiative often contain clauses that oblige the client country to partner with contractors from China, significantly limiting the potential to stimulate its domestic economy. Such a clause violates EU law which requires an open tender for the contractor. In addition, China's offer can hardly compete with alternative forms of funding offered within the EU, for example through the European Investment Bank.[8] For this reason, projects carried out so far within the 16+1 framework have focused predominantly on five non-EU countries and involved transport and energy infrastructures.

Taking into account the dynamics of centrifugal forces within the EU, one cannot rule out China's increased attempts to entrench its position in the region. The subsidisation of technologies or opening the Chinese market to imports from the CEE countries can be viewed as an attractive alternative to help maintain growth in case available EU funds are reduced, especially in view of the planned reduction of structural funds after 2020. The countries which joined the EU after 2004 are to a large extend the chief beneficiaries of those funds. Any adjustment of loan terms and conditions to the needs of the EU members participating in the 16+1 initiative can increase the competitiveness of Beijing's offering.

China's possible greater engagement with CEE entails a wide range of challenges. They not only refer to the strategic character of communication technologies which underpin security, but also to project implementation quality, cybersecurity standards, respecting privacy, and intellectual property protection. Despite the above limitations, cooperation with China within the Digital 3 Seas Initiative framework

6 http://en.ndrc.gov.cn/newsrelease/201503/t20150330_669367.html

7 http://www.china.org.cn/business/2017-05/23/content_40873203.htm

8 https://www.osw.waw.pl/pl/publikacje/komentarze-osw/2017-09-15/nietrafiona-oferta-pekinu-161-a-chinska-polityka-wobec-unii

is possible, but requires the above-mentioned issues to be addressed properly and to identify areas of mutually beneficial cooperation.

Imagine Central and Eastern Europe in 2035...

Constanța has become a dynamic regional hub for doing business and an attractive entrepreneurial city, one of the most innovative from Romania and CEE. Global ICT companies along with the academic innovation labs opened digital hubs in Constanța, as the city has already capitalized much of its great potential of being a hotspot of intelligent digital development. Companies like Google broadly support start-ups by offering a collaborative space for young entrepreneurs to accelerate their businesses and develop new skills, while partnering with local and regional SMEs. Constanța has partnered with many cities across CEE and provided a role model of digital economy and society growth, as a mature and creative community

CYBERSECURITY ON THE THREE SEAS INITIATIVE'S POLITICAL AGENDA

For many years, CEE countries (excluding Estonia) did not have a strong voice in the debate on cybersecurity, especially in terms of political solutions. The year 2017 did not bring expected outcomes following cybersecurity decisions that were made on the international arena. The lack of consensus within the 2016–2017 UN Group of Governmental Experts prompted the international community to seek an alternative space for discussion about the application of international law to cyber activities and the development of norms of responsible behaviour.

The Three Seas Initiative can take the opportunity and fill the gap. The countries of the region should actively engage in the debate on cybersecurity and give it a new momentum by becoming policy entrepreneurs. CEE has strong influence potential both on the continent and in the world and the countries of the region, exposed to digital conflicts and tensions can – and indeed should – contribute significantly to the discussion concerning the activities that help build stability and increase trust in this domain. Therefore, the Three Seas Initiative should play an important role in developing cybersecurity policies and strategic concepts, as well as in standardising processes, technologies and solutions. It is necessary to enter into a dialogue on priorities with other partners, including non-state actors. The place that regularly hosts the most prominent experts and policy-makers in the field during the annual European Cybersecurity Forum – CYBERSEC is Krakow, a city located in the heart of the region.

In 2019, Slovakia will chair OSCE and Romania will assume the Presidency of the Council of the European Union. It is a perfect time for the countries of the Three Seas Initiative to agree on their joint agenda for cybersecurity. One of the issues to address should be the implementation and development of the confidence-building measures (CBM) in cyberspace. One of the issues that the Digital 3 Seas Initiative should consider is the widening of the spectrum of activities of the Central European Cyber Security Platform (V4 states and Austria) in order to increase the cybersecurity of critical infrastructure. An important component of its joint activities should be stronger cooperation among CERTs.

The countries of the Digital 3 Seas Initiative should take advantage of their location on the eastern flank of the Alliance in order to set the tone for actions undertaken in response to hybrid threats. That should be done above all within B9 which is a format that focuses especially on security and defence matters in the region. Nevertheless, given that all members of the B9 forum participate in the Three Seas initiative, these issues are a matter of concern also for the Initiative to some extent.

The importance of developing a joint cyber deterrence strategy involving the cooperation of all members is significant. It is also justified by the fact that NATO competence centres specialised in this issue are located in the CEE region: the Cooperative Cyber Defence Centre of Excellence in Tallinn, the Counter Intelligence Centre of Excellence in Krakow, or the Strategic Communications Centre of Excellence in Riga, and Human Intelligence (HUMINT) Centre of Excellence in Oradea. Common actions under the Three Seas Initiative should be consistent with

latest decisions of NATO and the EU related to cyber defence, supporting their implementation as a coalition of countries that share the same risks. They should build on the existing *know-how* while leveraging their own technology. The project range should largely overlap with the scope PESCO defines as strengthening cyber defence capabilities through cooperation in three primary areas: information sharing, joint exercises and operational support. The PESCO project list includes two cyber defence initiatives: Cyber Threats and Incident Response Information Sharing Platform and Cyber Rapid Response Teams and Mutual Assistance in Cyber Security. The Three Seas countries should join them at least as observers.

A joint effort of the members of the Digital 3 Seas Initiative to strengthen the cybersecurity of the region should also include initiatives related to education, exchange of experts, training, exercises etc. In many cases, CEE states have very specific cybersecurity experiences (e.g. hybrid threats with an emphasis on multidimensional digital operations) on which they can draw to strengthen the competences of the entire international community.

Digital tools significantly strengthen the power and possibilities of influencing the audience. By influencing perception one can shape human emotions, opinions, and consequently – decisions and actions. In the era of ubiquitous digital tools, it is very easy to manipulate pictures, sound and videos. Given high viral potential of such 'fake' content, its use can be a very efficient method of information warfare. Western societies and governments may be unprepared for aggressive actions deployed against them below the threshold of war. That way, information warfare conducted in cyberspace may become a very attractive tool for conducting hybrid conflicts. The concepts of fake news and misinformation are no novelty. Despite what is commonly believed, it is not the U.S., but the CEE region (especially Ukraine and Poland) which first experienced information warfare consequences.

Together with East StratCom Task Force (EEAS) and Strategic Communications Centre of Excellence, the Digital 3 Seas countries should engage in combating disinformation campaigns by creating a platform to share experiences in the fight against disinformation and establishing a fund to support the development of expertise, analyses, and the publication of materials translated from the national languages of the Three Seas countries into English.

CONCLUSIONS

THE DIGITAL 3 SEAS INITIATIVE: BUILDING DIGITAL PARTNERSHIPS IN CENTRAL AND EASTERN EUROPE

CEE is becoming a critical region in the geopolitical power struggle between China and the U.S.

Dynamic digital transformation of CEE economies, an ever-increasing share of cyberspace in international relations and new, borderless hybrid security threats call for the Three Seas Initiative to be given a strong digital dimension, with cybersecurity component as its indispensable element.

'Plasticity' is a dominant characteristic of cyberspace which enables it to be shaped in a way that can increase the geostrategic and geostrategic importance of the CEE region and foster the development of the digital market-based economy and e-society (the free flow of data, e-commerce etc.).

Deepened cooperation in the region will reinforce the cohesion of the EU and the entire transatlantic community; it will also enhance the strategic presence of the U.S. in Europe.

Strong regional cooperation in all cyber issues, including energy security, is a future prerequisite for economic growth (digital interconnected economy) and security (common cyberthreats including disinformation) in CEE.

THE AIM OF THE INITIATIVE:

The Three Seas comprises 12 EU countries and 114 million of citizens dwelling upon the territory accounting for over 28 percent of the EU and generating GDP worth USD 1.6 trillion. The ever-changing global security architecture renders the region increasingly vital for actors as varied as the U.S., Great Britain, China or Russia. Upgrading the Three Seas Initiative by adding the digital and cybersecurity dimension to already existing ones: transportation and energy, may have geopolitical and geoeconomic consequences far beyond the CEE borders. Development of digital infrastructure in the face of 5G era, joint investments in state-of-the-art technologies such as IoT, blockchain and AI, deepen strategic and tactical cooperation to tackle cyberthreats and disinformation are in the core areas of the Digital 3 Seas Initiative.

PARTNERS OF THE DIGITAL 3 SEAS INITIATIVE:

GLOBSEC
IDEAS SHAPING THE WORLD

GLOBSEC is a global think-tank committed to enhancing security, prosperity and sustainability in Europe and throughout the world. Its mission is to influence the future by generating new ideas and solutions for a better and safer world. In an interconnected world, GLOBSEC stimulates public-private dialogue to shape agendas for the future. With global ambitions in mind, and building on its Central European legacy, GLOBSEC seeks to contribute to agendas which are critical for Europe. GLOBSEC acts in the spirit of European values and international cooperation. To this goal contributes the annual GLOBSEC Bratislava Forum, one of the leading conferences on global security in the world.

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

The Institute for Development and International Relations (IRMO) is a public, non-profit, scientific and policy research institute, engaged in the interdisciplinary study of European and international economic, political, cultural relations and communication. Founded in 1963 by the University of Zagreb and the Croatian Chamber of Commerce as the Africa Research Institute, the Institute has changed its name several times, reflecting the changes in scholarly focus. The fundamental mission of the Institute is developing and disseminating theoretical, methodological and technical knowledge and skills required for the scientific and professional interpretation and evaluation of contemporary international relations which affect various human activities and related developmental trends important for the Republic of Croatia. Development tendencies are observed in the local, regional, European and global context. The Institute has 44 employees out of which 16 are tenured academic staff and 7 are doctoral or postdoctoral researchers.

NEW STRATEGY CENTER

New Strategy Center is a Romanian think-tank specialising in foreign, defense, and security policy, a self-financed, non-profit, non-partisan, non-governmental organisation. New Strategy Center operates at three main levels: providing analytical inputs and expert advice to decision makers; holding regular debates, both in-house and public, on subjects of topical interest; expanding external outreach through partnerships with similar institutions and organisations in Europe and the US, joint policy papers and international conferences. The Black Sea and the Balkans space in the vicinity of Romania are priority areas of interest for New Strategy Center in terms of security concerns and emerging opportunities for bilateral and multilateral cooperation. The current activities of New Strategy Center also cover such subjects as domestic developments in Romania as relevant for national security, military modernisation and national defense procurement, energy security and the promises of new technologies, non-conventional and hybrid threats, including cyberspace, and public diplomacy.

The Kosciuszko Institute is a non-profit, independent, non-governmental research and development institute (think tank), founded in 2000.

The Kosciuszko Institute's aim is to influence the socio-economic development and the security of Poland as a new member of the EU and a partner in the Euro-Atlantic alliance. Studies conducted by the Institutes have been the foundation for both important legislative reforms as well as a content-related support for those responsible for making strategic decisions.

The Kosciuszko Institute organizes the European Cybersecurity Forum – CYBERSEC – the first conference of its kind in Poland and one of just a few regular public policy conferences devoted to the strategic issues of cyberspace and cybersecurity in Europe, and also publishes the European Cybersecurity Journal – a new specialised quarterly publication devoted to cybersecurity.

Office: Wilhelma Feldmana 4/9-10, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: instytut@ik.org.pl

More on the European Cybersecurity Forum: http://cybersecforum.eu/

More on the European Cybersecurity Journal: http://cybersecforum.eu/en/about-ecj/

PARTNERS OF THE DIGITAL 3 SEAS INITIATIVE:

GLOBSEC
IDEAS SHAPING THE WORLD

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

NEW STRATEGY CENTER

FOUNDER OF THE DIGITAL 3 SEAS INITIATIVE:

THE KOSCIUSZKO INSTITUTE