Czerwiec 2018

INSTYTUT KOŚCIUSZKI

BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI

THE DIGITAL 3 SEAS INITIATIVE

INICJATYWA CYFROWEGO TRÓJMORZA TO KROK W PRZYSZŁOŚĆ REGIONU

STRESZCZENIE

Pojawienie się cyberprzestrzeni zmieniło paradygmat funkcjonowania współczesnych państw. Powstała nowa arena dla działań poszczególnych podmiotów, których nie ogranicza już geografia. Cyberprzestrzeń stała się kolejną determinantą geostrategicznego i geoekonomicznego znaczenia państw.

Autorzy poniższego opracowania postulują szereg działań na rzecz budowania współpracy regionalnej w wymiarze cyfrowym w Europie Środkowo-Wschodniej pod nazwą „Inicjatywy Cyfrowego Trójmorza", która obejmowałaby m.in.

1) **Wzmocnienie wymiaru cyfrowego w ramach Inicjatywy Trójmorza z uwzględnieniem cyberbezpieczeństwa w trzech filarach: energetycznym, transportowym i cyfrowym.**

2) **Wspólne projekty dotyczące infrastruktury transgranicznej** (np. *3 Seas Digital Highway*) umożliwiające lepszy i bezpieczniejszy transfer danych z północy na południe regionu i zniwelowanie różnic w infrastrukturze telekomunikacyjnej, w tym sieci światłowodów, infrastruktury technologii 5G, wysp danych, uzupełniając w ten sposób infrastrukturę energetyczną i transportową powstałą w ramach Inicjatywy Trójmorza;

3) Wspólne inicjatywy odpowiadające **wyzwaniom cyfrowej transformacji regionu Trójmorza w zakresie integracji obecnej infrastruktury z nowymi technologiami i rozwiązaniami** (np. strategiczne i operacyjne wyzwania dotyczące integracji chmury obliczeniowej w ramach sektora publicznego i prywatnego);

4) Wypracowanie **wspólnych modeli bezpieczeństwa i standardów związanych z budową sieci 5G**, opartych na zasadzie *security by design;*

5) Opracowanie i wdrożenie polityki **swobodnego przepływu danych nieosobowych**, która leży u podstaw innowacyjnego przemysłu opartego na danych oraz przełomowych technologii (np. sztuczna inteligencja, Internet rzeczy);

6) **Wspólne inicjatywy technologiczne** w celu wzmocnienia transgranicznej współpracy edukacyjnej i przemysłowych badań naukowych dotyczących np. autonomicznego transportu, infrastruktury elektromobilności, inteligentnych rozwiązań dla miast, blockchain, i tym samym przyspieszenia transformacji cyfrowej w Europie Środkowo-Wschodniej (EŚW);

ISSN 1689-9873

7) Wsparcie **rozwoju wybranych sektorów Przemysłu 4.0**, takich jak fin-tech, cyberbezpieczeństwo, elektromobilność czy health-tech, które już dają przewagę komparatywną EŚW na globalnym rynku;

8) Wzmocnienie i zabezpieczenie **centrów e-handlu** w miejscach o strategicznym znaczeniu dla całego regionu, poprzez budowę inteligentnych magazynów oraz inteligentnych systemów odprawy celnej;

9) Współpraca w dziedzinie bezpieczeństwa w celu **przeciwdziałania wojnie informacyjnej**, oparta na wspólnym doświadczeniu i podyktowana wysoką ekspozycją regionu na zagrożenia hybrydowe;

10) Stymulowanie współpracy, integracji i zaufania pomiędzy **cyfrowymi ośrodkami innowacji, centrami kompetencji** oraz globalnymi i regionalnymi firmami (np. tworzenie platform współpracy, wzrost popularyzacji innowacji cyfrowych, promowanie dojrzałych technologii opartych na potrzebach przemysłu);

11) Zwiększenie zaangażowania w regionie prowadzącego do **opracowania polityk cyberbezpieczeństwa** i koncepcji strategicznych na poziomie europejskim.

WPROWADZENIE DO KONCEPCJI

Góry, morza i rzeki, które stanowią o uroku półwyspu europejskiego, doprowadziły do powstania równie zróżnicowanego krajobrazu politycznego i ekonomicznego. Geografia była i wciąż jest czynnikiem decydującym o potencjale ekonomicznym państw, lokalizacji centrów przemysłowych, kształcie sojuszy czy przebiegu granic. Jest to szczególnie widoczne w Europie Środkowo-Wschodniej.

Podejście państw regionu do cyberprzestrzeni ukształtuje cyfrową mapę Europy w XXI wieku. Możemy odtworzyć stare linie geograficznych podziałów, albo zbudować infrastrukturę, która będzie pogłębiać współpracę. Przyszłość Europy zależeć będzie od powodzenia wspólnych transgranicznych projektów infrastrukturalnych, postępów w zakresie transformacji cyfrowej i skutecznych modeli współpracy na poziomie wewnątrzkrajowym, jak i między państwami i sektorami. Możemy narysować mapę cyfrową, na której znajdą się albo nowoczesne państwa europejskie połączone cyfrowymi rzekami, którymi odbywa się swobodny przepływ danych. W przeciwnym razie, mapa ta stanowić będzie zbiór wyobcowanych państw, izolujących się w obrębie własnych granic. Powodzenie tego procesu ma znaczenie nie tylko dla państw regionu, ale także dla spójności UE i całej wspólnoty transatlantyckiej.

CZYM JEST INICJATYWA CYFROWEGO TRÓJMORZA?

Inicjatywa Cyfrowego Trójmorza to zbiór projektów transgranicznych i inicjatyw mających na celu rozwój infrastruktury cyfrowej, wspólnych inwestycji i prac badawczo-rozwojowych, a także koncepcji politycznych i legislacyjnych realizowanych na poziomie UE. Głównym pomysłem jest połączenie koncepcji ***security by design*** z transformacją cyfrową sektora publicznego i prywatnego. Inicjatywa Cyfrowego Trójmorza opiera się na sieciach infrastruktury transportowej i energetycznej, które stanowią trzon Inicjatywy Trójmorza i uzupełnia go o wymiar cyber.

CZYM JEST INICJATYWA TRÓJMORZA?

Trójmorze (ang. Three Seas Initiative, 3SI) jest projektem gospodarczo-politycznym zainaugurowanym w 2016 r., który ma na celu pogłębienie integracji państw Europy Środkowo-Wschodniej oraz wzmocnienie ich pozycji w Unii Europejskiej.

DLACZEGO JEST ISTOTNA?

Trójmorze to 12 krajów UE, 114 milionów obywateli zamieszkujących ponad 28 procent terytorium UE i wytwarzających PKB na poziomie 1,6 bilionów dolarów.

Nieustannie zmieniająca się globalna architektura bezpieczeństwa sprawia, że Trójmorze odgrywa coraz większe znaczenie dla aktorów takich jak USA, Wielka Brytania, Chiny czy Rosja. Sposób, w jaki infrastruktura Trójmorza łączy się ze światem będzie mieć geopolityczne konsekwencje, które wykraczają daleko poza granice regionu.

Trójmorze jest szczególnie istotne dla USA, które będzie dążyć do ograniczenia wpływów chińskiej Inicjatywy Pasa i Szlaku (ang. Belt and Road Initiative),

wraz z tzw. Cyfrowym Jedwabnym Szlakiem. Poprzez format 16+1 Chiny starają się realizować europejską część Pasa i Szlaku, a położenie geograficzne EŚW ma kluczowe znaczenie dla budowy połączeń między Europą a Dalekim Wschodem.

Inicjatywa Cyfrowego Trójmorza ma ogromny potencjał jeśli chodzi o budowanie synergii z projektami takimi jak Jednolity rynek cyfrowy (ang. Digital Single Market), w obrębie normatywnych granic i ram ustalonych przez UE.

MAPA INICJATYWY CYFROWEGO TRÓJMORZA – BEZPIECZNA INFRASTRUKTURA CYFROWA I INTELIGENTNE POLITYKI

- ***3 Seas Digital Highway*** przewiduje budowę infrastruktury światłowodowej i 5G wzdłuż już zaplanowanych dróg transportowych i linii energetycznych;
- Ośrodki oferujące usługi bazujące na **chmurze obliczeniowej** i **przechowywaniu danych**, tzw. **wyspy danych**, mogłyby powstawać wzdłuż ***3 Seas Digital Highway***;
- **Swobodny przepływ danych** wyeliminowałby konieczność dublowania infrastruktury mającej na celu magazynowanie zasobów cyfrowych, łącząc w ten sposób **wyspy danych** w całym regionie i stwarzając odpowiednie warunki dla rozwoju gospodarki opartej na danych;
- Usprawniona i bezpieczna infrastruktura telekomunikacyjna wraz z inteligentnymi systemami magazynowania i odprawy celnej mogłyby ułatwić tworzenie **ośrodków e-handlu** w pobliżu węzłów komunikacyjnych.

WDROŻENIE INICJATYWY CYFROWEGO TRÓJMORZA – PLAN DZIAŁANIA NA 2018 R.:

- **Angażowanie do współpracy think tanków i ekspertów** z regionu, USA i Wielkiej Brytanii;
- Zainicjowanie **Digital 3 Seas Business Forum**;
- Opracowanie szczegółowej **strategii wdrażania** komponentu cyfrowego jako części Inicjatywy Cyfrowego Trójmorza;
- Promowanie inicjatywy na **konferencji CYBERSEC 2018 w Krakowie** (8–9 października 2018);
- Poparcie dla pomysłu oficjalnego włączenia komponentu cyfrowego do Inicjatywy Trójmorza w trakcie **szczytu państw Trójmorza w Rumunii** (jesień 2018).

INICJATYWA TRÓJMORZA

Trójmorze (ang. Three Seas Initiative, 3SI) jest projektem gospodarczo-politycznym, który ma na celu pogłębienie integracji państw Europy Środkowo-Wschodniej oraz wzmocnienie ich pozycji w Unii Europejskiej (UE) i NATO. Celem Inicjatywy Trójmorza zainaugurowanej w sierpniu 2016 r. przez prezydenta RP, Andrzeja Dudę oraz prezydent Chorwacji, Kolindę Grabar-Kitarovic jest stymulowanie wielowymiarowej współpracy, szczególnie w obszarze gospodarki i infrastruktury. Inicjatywa Trójmorza obejmuje 12 krajów UE, 22 procent jej obywateli zamieszkujących ponad 28 procent terytorium UE i wytwarzających PKB na poziomie 1,6 bilionów dolarów.

Powołanie Inicjatywy Trójmorza oraz Bukaresztańskiej Dziewiątki (B9), inicjatywy współpracy krajów tzw. wschodniej flanki NATO, podobnej w założeniach i zasięgu terytorialnym do Trójmorza, jest dowodem na wzrastającą potrzebę stworzenia mocnych ram regionalnej współpracy w UE.

Dynamiczna transformacja cyfrowa gospodarek EŚW, coraz istotniejszy udział cyberprzestrzeni w relacjach międzynarodowych oraz nowe transgraniczne zagrożenia bezpieczeństwa o charakterze hybrydowym wymagają nadania Inicjatywie Trójmorza silnego wymiaru cyfrowego, którego nieodzownym elementem jest komponent cyberbezpieczeństwa.

Zagrożenia w regionie EŚW i pozostałej części Europy do pewnego stopnia posiadają wspólny mianownik, jednak region EŚW jest też dodatkowo poligonem, na którym testuje się kampanie hybrydowe. Państwa EŚW, podobnie jak każdy inny region na świecie, padają ofiarą różnych form cyberataków. Jednak szczególnym zagrożeniem dla nich są konwencjonalne konflikty, którym coraz częściej towarzyszą złowrogie działania w cyberprzestrzeni, co wynika z ich lokalizacji w napiętym geopolitycznie regionie. Kraje EŚW, które są członkami NATO, zdecydowanie opowiadają się za wzmocnieniem obecności NATO w regionie, postrzegając ją jako gwaranta ich bezpieczeństwa. Obecnie konwencjonalny i otwarty konflikt militarny jest mało prawdopodobny ze względu na zbyt wysoki poziom ryzyka związany z jego podjęciem.

Jednak państwa EŚW są niezwykle narażone na szereg operacji prowadzonych w cyberprzestrzeni, które nie tylko wiążą się z przeprowadzaniem cyberataków na systemy IT czy OT, ale także zawierają element walki psychologicznej. Historia pokazała, że wiele cyberataków, zwłaszcza tych mających na celu naruszenie bezpieczeństwa narodowego, po raz pierwszy zostały przeprowadzone w regionie EŚW (np. zakrojony na dużą skalę cyberatak na Estonię, kampanie dezinformacyjne w Polsce itp.).

Inicjatywa Cyfrowego Trójmorza ma potencjał wspierania wspólnych transgranicznych projektów technologicznych, koncepcji politycznych i legislacyjnych na szczeblu UE, a także współpracy naukowej i edukacyjnej oraz rozwoju bezpiecznej infrastruktury cyfrowej. Silna współpraca regionalna jest niezbędna do tego, by przyspieszyć tempo i charakter globalnych cyfrowych zmian. Aby mniejsze kraje mogły dołączyć do grupy cyber supermocarstw muszą zaangażować swoje zasoby w obrębie dobrze zorganizowanych ram współpracy.

Inicjatywę Cyfrowego Trójmorza należy postrzegać jako komplementarną i wpisującą się w istniejące projekty unijne, takie jak Jednolity rynek cyfrowy oraz instrument „Łącząc Europę" (ang. Connecting Europe Facility). Członkowie projektu powinni ściśle współpracować z partnerami z UE oraz NATO. Sojusznicy powinni także postrzegać Inicjatywę jako wyjątkowe źródło wiedzy na temat przyszłych zagrożeń, gdyż to, co dzisiaj dzieje się w cyberprzestrzeni w tym regionie, jutro najprawdopodobniej dotknie ich kraje.

Inicjatywa Trójmorza jest koncepcją definiującą przyszłość EŚW w nadchodzących dekadach i jest strategicznie wspierana przez USA

„Inicjatywa Trójmorza nie tylko pozwoli waszym obywatelom doskonale się rozwijać, ale także zapewni waszym krajom suwerenność, bezpieczeństwo i wolność od zagranicznych nacisków. Narody Trójmorza staną się silniejsze niż kiedykolwiek wcześniej. Wraz z siłą waszych krajów rośnie siła wszystkich wolnych narodów Europy i całego Zachodu."
Prezydent USA Donald Trump w przemówieniu do przywódców krajów Trójmorza na szczycie państw Trójmorza w Warszawie 6 lipca 2017 r.

„Ważnym elementem strategii USA jest zachęcanie do zacieśnienia współpracy politycznej i gospodarczej na szczeblu regionalnym, między sojusznikami, którzy są najbardziej podatni na manipulację dostawami [surowców] w Europie Środkowo-Wschodniej. Lekceważenie konieczności rozbudowy infrastruktury w kierunku północ-południe, między Morzem Bałtyckim a Morzem Czarnym, było i jest czynnikiem przyczyniającym się do słabości geopolitycznej Europy na Wschodzie. Priorytetem USA będzie nasze zaangażowanie w działalność regionalnych partnerstw, takich jak Inicjatywa Trójmorza, Grupa Wyszehradzka, Bukaresztańska Dziewiątka i Grupa Nordycko-Bałtycka stanowiących platformy służące wzmocnieniu odporności regionu na działania wykorzystujące energetykę jako formę nacisku."
A. Wess Mitchell, Asystent Sekretarza Stanu ds. Europy i Eurazji, Komisja Spraw Zagranicznych Senatu, Podkomisja ds. Europy oraz Bezpieczeństwa i Współpracy w Regionie, 12 grudnia 2017 r.

INICJATYWA TRÓJMORZA I JEJ MIĘDZYNARODOWY KONTEKST

Ostatnie lata przyniosły wyraźne zmiany na geopolitycznej szachownicy wpływów. Na naszych oczach swoje oblicze zmienia UE. W okresie niepewności związanej ze słabym rozwojem gospodarczym Wspólnoty, kryzysem imigracyjnym i wzrostem tendencji odśrodkowych, których odzwierciedleniem był Brexit, potrzebne są nowe impulsy, które powstrzymają jej dalszą dekompozycję. Konieczne są koncepcje reintegrujące partnerów unijnych wokół nowych projektów i przedsięwzięć. Powinny one być skoncentrowane na realizacji wspólnych interesów poszczególnych krajów, budować ich przewagi polityczne i gospodarcze, jednocześnie przyczyniając się do osiągnięcia celów polityk unijnych. Ponieważ nie może być silnej UE bez silnej EŚW, w zmieniającej się rzeczywistości Inicjatywa Trójmorza uzupełniona o wymiar cyfrowy ma niewątpliwie szansę wpisać się w realizację tego postulatu.

Podczas gdy Wielka Brytania po Brexicie będzie dążyć do ustanowienia stosunków dwustronnych z państwami członkowskimi UE, podjęcie ściślejszej współpracy z państwami Trójmorza wydaje się naturalnym kierunkiem jej działań. Z drugiej strony współpraca z krajami EŚW może stanowić ważne ogniwo utrzymania strategicznej obecności Stanów Zjednoczonych w Europie, stając się gwarantem kontynuacji propagowania idei transatlantyckiej.

EŚW nabiera kluczowego znaczenia w geopolitycznej rywalizacji pomiędzy Chinami a Stanami Zjednoczonymi. Wielki geopolityczny projekt Chin – Inicjatywa Pasa i Szlaku – traktuje EŚW jako „bramę do Europy". Chiny dostrzegają znaczenie tego regionu i próbują wzmacniać swoje wpływy polityczno-gospodarcze w tej części Europy. Główną platformą tych działań jest CEEC Forum, zwane także „16+1". Projekt ten zainaugurowany w 2012 r. skupia 16 krajów regionu EŚW, w tym 11 krajów członkowskich UE.

Nie można zapominać, że sąsiadujące z Rosją kraje EŚW, stanowią granicę zewnętrzną UE i NATO. Wobec agresywnej polityki Moskwy, zarówno w wymiarze konwencjonalnym (konflikt zbrojny na Ukrainie, operacja ekspedycyjna w Syrii, wznowienie patroli bombowców strategicznych i okrętów podwodnych z napędem jądrowym, wzmocnienie i modernizacja tak zwanej triady nuklearnej, wielkoskalowe ćwiczenia wojskowe z wykorzystaniem dużych ugrupowań

wojsk powietrzno-desantowych i lotnictwa strategicznego, doktryna wojskowa uznająca pozostawanie Rosji w stanie permanentnego konfliktu), a także cyfrowym (wpływanie na przebieg kampanii wyborczych w USA i Francji, sponsorowanie i inspirowanie cyberataków, cyberszpiegostwo, mniej lub bardziej otwarty rozwój ofensywnych zdolności do prowadzenia działań zbrojnych w cyberprzestrzeni, wykorzystywanie narzędzi cybernetycznych w działaniach hybrydowych), ma olbrzymie konsekwencje strategiczne i ekonomiczne.

Z tych wszystkich powodów EŚW jest newralgicznym punktem na geopolitycznej mapie XXI wieku. Dzięki projektom wspólnie realizowanym w ramach Inicjatywy Cyfrowego Trójmorza, region może uzyskać kolejną przewagę konkurencyjną i stać się siłą napędową rozwoju gospodarczego UE oraz ważnym elementem nowej globalnej architektury bezpieczeństwa.

EŚW jest newralgicznym punktem na geopolitycznej mapie XXI wieku.

THE 3 SEAS DIGITAL HIGHWAY

Aktualna koncepcja Trójmorza przewiduje przede wszystkim rozbudowę infrastruktury energetycznej i transportowej w celu połączenia północy i południa regionu. Koncepcję należy jednak rozszerzyć o element związany z bezpieczną transmisją danych. Trójmorze powinno zostać połączone tzw. *3 Seas Digital Highway*. W 2015 r. do użytku oddano światłowód Baltic Highway, łączący Tallinn z Frankfurtem przez Rygę, Wilno, Warszawę i Berlin. Jak większość podobnych projektów inwestycyjnych ma on na celu połączenie Europy Zachodniej ze Wschodnią. Projekt Trójmorza, łączący Bałtyk, Adriatyk oraz Morze Czarne, powinien uwzględniać jako swoją nieodłączną część rozbudowę infrastruktury cyfrowej także na linii północ-południe. Pozwoli to na uzupełnienie mapy połączeń cyfrowych stanowiących aktualnie fundament zmieniających się cyfrowo gospodarek. Koncepcja uzupełnienia infrastruktury gazowej i drogowej budowanej w ramach projektów Trójmorza o komponent cyfrowy powinna zostać dopracowana i obejmować swoim zasięgiem wszystkie państwa Inicjatywy. Synergia ta pozwoli skrócić czas wymagany do przeprowadzenia procesu inwestycyjnego, a także obniżyć koszty przedsięwzięcia.

Budowa *3 Seas Digital Highway* może pomóc w rozwoju nowoczesnej technologii bezprzewodowej 5G i całego opartego na niej ekosystemu, wspólnego dla krajów EŚW. Oczekuje się, że system komórkowy piątej generacji, będący platformą łączącą w elastyczny sposób różne technologie radiowe i mającą parametry techniczne dostosowane do realizowanych usług końcowych, zrewolucjonizuje telekomunikację mobilną i zapewni szeroki dostęp do nowych technologii mobilnych nie tylko obywatelom, ale także przedsiębiorstwom, zwłaszcza tym wpisującym się w koncepcję Przemysłu 4.0., które mogą na nim zbudować swoją przewagę konkurencyjną. Polska jest jednym z krajów regionu, które inwestują w rozbudowę sieci komórkowych z uwzględnieniem kolejnych wersji standardów, a tym samym w koncepcję „mobilnego państwa" i gospodarki opartej na danych – „Przemysł +". Dostęp do szybkiego Internetu realizowany dziś przez stacje bazowe sieci komórkowej 4G (LTE i LTE-Advanced), a w przyszłości sieci 5G, w dużej mierze podłączonych do sieci światłowodowych, to podstawa rozwoju gospodarki e-społeczeństwa bazującego na rynku cyfrowym (swobodnym przepływie danych, e-handlu itd.). Szybki Internet to także szansa na stworzenie lepiej zintegrowanego systemu powiadamiania i zarządzania kryzysowego. Sieć światłowodów, budowana zarówno w obszarze szkieletowym, jak i dostępowym, uzupełniona o technologię 5G, pomogłaby zniwelować luki infrastruktury komunikacyjnej EŚW wobec krajów UE15. Pozwoliłoby to na dalsze pogłębienie cyfrowej współpracy w całej Europie, wpływając znacząco na konkurencyjność regionu i realizację założeń Jednolitego rynku cyfrowego. Dodatkowo szkielet takiej międzynarodowej sieci światłowodowej pozwoliłby na wymianę wzrastającego ruchu roamingowego, czy to na poziomie samego dostępu do Internetu, czy też realizacji usług specjalistycznych w sieciach 5G, np. pionowej wymiany danych pomiędzy zlokalizowanymi w różnych krajach fabrykami działającymi zgodnie z koncepcją Przemysłu 4.0.

Budowa *3 Seas Digital Highway* niesie za sobą konieczność zadbania o bezpieczeństwo danych. Światłowody znajdują się nie tylko pod ziemią i na jej powierzchni, ale biegną też po dnach oceanów i mórz. Choć taka lokalizacja skutecznie utrudnia

prowadzenie podsłuchu światłowodów, jest on jednak możliwy w punktach węzłowych. Udane ataki na infrastrukturę światłowodową mogą prowadzić do odcięcia kraju od globalnej sieci internetowej. Zapewnienie odporności podmorskiej i lądowej infrastruktury światłowodowej na uszkodzenia oraz na nowe zagrożenia wymaga odpowiedniego szyfrowania i nadzoru poprzez odpowiednie systemy i procedury. Ze względu na kluczową rolę regionu jako wschodniej flanki NATO, zwłaszcza w obliczu rosnącej aktywności rosyjskich bezzałogowych pojazdów podwodnych w pobliżu podwodnych kabli światłowodowych, kwestia ta powinna znaleźć się wysoko na politycznej agendzie Inicjatywy Cyfrowego Trójmorza.

Z kolei, aby zbudować zaufanie obywateli i przemysłu do 5G, potrzebne jest uwzględnienie komponentu cyberbezpieczeństwa w całej wielowarstwowej architekturze sieci piątej generacji, którą, oprócz wysokich parametrów technicznych, cechować powinna przede wszystkim niezawodność i integralność. Stąd ważne jest „kompleksowe podejście do bezpieczeństwa 5G, nie tylko na poziomie zapewnienia usług sieciowych, ale także w warstwach wyższych związanych ze świadczeniem konkretnych usług”[1]. Aby spełnić ten warunek, konieczne jest opracowanie kryteriów wyboru podwykonawców, w tym operatorów usług telekomunikacyjnych, dostawców usług chmurowych, wertykalnych i wirtualnych prywatnych sieci 5G. Dyskusja na ten temat rozpoczęła się już w Stanach Zjednoczonych, które rozważają wyłączenie niektórych firm z możliwości uczestniczenia w procesie inwestycyjnym ze względów bezpieczeństwa. Stany Zjednoczone chcą w tym zakresie ściśle współpracować ze swoimi sojusznikami. Wraz z rosnącą popularnością technologii 5G na całym świecie można więc założyć, że wypracowanie wspólnych modeli bezpieczeństwa i dobrych praktyk związanych z budową sieci 5G może odbyć się nie tylko na powołanych w tym celu forach międzynarodowych, ale także w ramach Inicjatywy Cyfrowego Trójmorza.

1 Ministerstwo Cyfryzacji, Strategia 5G dla Polski, s. 35

WYOBRAŹ SOBIE EUROPĘ ŚRODKOWO-WSCHODNIĄ W 2030…

Wyobraź sobie flotę elektrycznych, autonomicznych pojazdów poruszających się po Krakowie – do niedawna jednym z najbardziej zanieczyszczonych i zatłoczonych miast w Europie. Kiedy pierwsze autonomiczne samochody do użytku mieszkańców pojawiły się na ulicach miasta w 2025 r., nikt nie przypuszczał, że technologia ta będzie w stanie podnieść jakość życia w mieście w tak krótkim czasie. Jednak samorządowy projekt zainaugurowany w 2020 r. miał wszelkie prawa powodzenia. Już na tym etapie miasto było doskonale rozwijającym się „living lab” bezpiecznych rozwiązań „smart city” z dynamicznie implementowaną infrastrukturą 5G. Już na etapie projektu włączono w kalkulacje korzystanie z nowoczesnych „data centres” w Czechach i na Słowacji. Dostęp do nich umożliwiły transgraniczne połączenia światłowodowe o wysokiej przepustowości, które zaczęły pokrywać terytorium EŚW wraz z rozwojem infrastruktury 5G. Było to kluczowe dla powodzenia projektu, który byłby nierentowny, jeśli zostałby oparty o usługi zewnętrznych partnerów. Byłby również niemożliwy, gdyby nie swobodny przepływ danych, który znacznie uprościł prace na dużych ilościach danych w projekcie tak ambitnym, jak flota autonomicznych samochodów.

WYMIAR EKONOMICZNY INICJATYWY CYFROWEGO TRÓJMORZA

Budowa nowoczesnej, solidnej i bezpiecznej infrastruktury technologicznej może być zachętą dla strategicznych inwestycji krajowych i zagranicznych, wspierać rozwój i umocnić pozycję przedsiębiorstw działających w regionie. Skorzystają one z możliwości zwiększenia swojego udziału na rynkach krajów będących stronami porozumienia, a także, dzięki łatwiejszej wymianie informacji i *know-how*, doświadczą technologicznego efektu *spill-over*, – transferu wiedzy i umiejętności do obszarów, gdzie wciąż występuje luka technologiczna.

Wzdłuż *3 Seas Digital Highway* powinny powstać tzw. „wyspy danych” (ang. data islands) będące hubami dla usług opartych na chmurach obliczeniowych oraz przechowywaniu danych. Może to stanowić

bodziec dla współpracy publiczno-prywatnej opartej na budowaniu bezpiecznej gospodarki cyfrowej. Tego typu ośrodki przyczynią się do powstania nowych oraz umocnienia już istniejących regionalnych centrów innowacji cyfrowych[2] (ang. Digital Innovation Hub, DIH) mających na celu wspieranie rozwoju Przemysłu 4.0 poprzez aktywizację współpracy pomiędzy jednostkami naukowymi, przedsiębiorcami oraz sektorem publicznym. *3 Seas Digital Highway,* wraz z siecią połączonych ze sobą hubów, przyspieszy transformację cyfrową gospodarek regionu, zwiększając znaczenie EŚW w ramach unijnej agendy Przemysł 4.0 oraz centrów innowacji cyfrowych. Konieczne jest również podjęcie dyskusji na temat tego, jak sprostać wyzwaniom w zakresie integracji obecnej infrastruktury z nowymi technologiami i rozwiązaniami, które znacząco utrudniają cyfrową transformację regionu Trójmorza (np. strategiczne i operacyjne wyzwania dotyczące Integracji chmury obliczeniowej w ramach sektora prywatnego i publicznego).

Rozbudowana infrastruktura teleinformatyczna umożliwi także stworzenie centrów e-handlu w strategicznych dla całego regionu lokalizacjach w celu ułatwienia eksportu przedsiębiorcom. Takim miejscem może być będący w realizacji Centralny Port Komunikacyjny mający powstać w geograficznym centrum Europy, pomiędzy Warszawą a Łodzią, lub węzeł transportowy zlokalizowany w Konstancy – największym porcie morskim nad Morzem Czarnym[3]. Ich celem jest integracja węzłów transportu kolejowego, drogowego i lotniczego. Powstanie zaplecza o tak silnych zaletach logistycznych stanowić będzie doskonały ekosystem dla rozwoju ułatwień dla e-handlu, takich jak budowa inteligentnych magazynów oraz systemu inteligentnej obsługi celnej. W celu skutecznego rozwoju inicjatyw związanych z elektronicznymi usługami oraz cyfryzacją procesów logistycznych niezbędne jest stworzenie solidnych podstaw cyberbezpieczeństwa zapewniających zaufanie pomiędzy przedsiębiorcami a dostawcami wyżej wspomnianych usług. Tylko przejrzyste i niezawodne narzędzia będą w stanie efektywnie przyczynić się do ułatwienia procesów handlowych, a co za tym idzie – rozwoju samego e-handlu.

Innowacyjne środowisko ICT w ramach powstałych centrów e-handlu może przyczynić się do rozwoju szeregu rozwiązań opartych na sztucznej inteligencji oraz Internecie rzeczy, które do skutecznej implementacji wymagają kreatywnego i chłonnego technologicznie otoczenia, a także świadomego szans i zagrożeń społeczeństwa. Można więc spodziewać się dynamicznego rozwoju autonomicznego transportu, odpowiedniej dla elektromobilności infrastruktury oraz inteligentnych rozwiązań dla miast i wsi, takich jak inteligentne sieci elektroenergetyczne (ang. smart grids), w tym rozproszone systemy energetyczne, inteligentne systemy oświetlenia, ruchu drogowego, systemy zapewniające bezpieczeństwo mieszkańcom, a nawet nadzorujące pola uprawne. Z uwagi na silne powiązanie skuteczności i efektywności tego typu rozwiązań z przesyłem danych w czasie rzeczywistym (ang. real-time data), potrzebują one bezpiecznego i nowoczesnego zaplecza sieciowego, którym w założeniach mają być sieci 5G.

Cyfrowy rozwój Europy nie jest możliwy bez swobodnego przepływu danych (ang. free flow of data) w wymiarze transgranicznym. Niweluje on konieczność przechowywania zasobów cyfrowych w wielu miejscach, co redukuje potrzebę powielania nakładów na systemy informatyczne, optymalizując związane z tym koszty. Swobodny przepływ danych ma kluczowe znaczenie dla rozwoju gospodarki opartej na danych (ang. data-driven economy), stymulując między innymi tworzenie nowych produktów oraz usług wykorzystujących zasoby, takie jak bazy otwartych danych czy zbiory „big data". Jest to kwestia szczególnie ważna dla konkurencyjności małych i średnich przedsiębiorstw. Należy nadmienić, że kraje Trójmorza powinny stać się aktywnymi członkami europejskiej inicjatywy High-Performance Computing (HPC).

Ostatnie lata to znaczny rozwój sceny start-upowej w EŚW. Rewolucja związana z cyfryzacją gospodarek okazała się wielką szansą dla innowacji opartych na solidnych technologicznych i inżynieryjnych

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

3 Konstanca znajduje się u zbiegu trzech transeuropejskich korytarzy transportowych i handlowych (Korytarz IV, IX i naddunajski VII).

podstawach wypracowywanych w ośrodkach akademickich regionu. Kolejnym kluczowym krokiem powinno być wsparcie dla rozwoju wybranych sektorów Przemysłu 4.0, takich jak fin-tech, cyberbezpieczeństwo, elektromobilność czy health-tech, które już stanowią przewagę komparatywną EŚW na globalnym rynku. Ze względu na efekt skali oraz problem niedostatecznej wielkości rynków wewnętrznych poszczególnych krajów, dedykowane programy akceleracyjne powinny objąć swoim zasięgiem cały region, stając się platformą dla ekspansji lokalnej i globalnej uczestniczących w nich start-upów.

Inicjatywa Cyfrowego Trójmorza może stać się globalnym pionierem odpowiedzialnego wykorzystania technologii rozproszonych rejestrów takich jak blockchain, będącej zarówno systemem transakcyjnym, jak i technologią przechowywania danych. Mechanizmy kryptograficzne zastosowane w technologii blokchain chronią zapisane informacje, które, co do zasady, nie mogą zostać zmienione ani usunięte. Przykładem zastosowania tej technologii może być utworzenie własnej kryptowaluty[4], zarządzanie łańcuchem dostaw w blockchain, stworzenie rozproszonych (przez co dużo bezpieczniejszych) baz danych, czy zastosowanie inteligentnych umów (ang. smart contracts) na potrzeby ochrony własności intelektualnej. Dodatkowo jedną z zalet technologii jest możliwość dezintermediacji – usunięcia z łańcucha dostaw pośredników. Takie działanie może pomóc w budowie usług bazujących na bezpośredniej relacji pomiędzy państwami EŚW a ich obywatelami w ramach Inicjatywy Cyfrowego Trójmorza. Przykładem mógłby być system poboru opłat bazujący wyłącznie na aplikacji mobilnej, mapach cyfrowych i technologii rozproszonych rejestrów. Prostota i nowatorska koncepcja mogłaby pomóc w kolejnym kroku w ekspansji rozwiązania na pozostałe kraje UE.

Potencjał technologii blockchain jest obecnie dostrzegany w niemal wszystkich sektorach gospodarki. Jedynie w ciągu pierwszych 9 miesięcy 2016 r. start-upy wykorzystujące technologię blockchain przyciągnęły inwestycje rzędu 1,4 miliardów dolarów[5].

Wszystkie te inicjatywy przyczynią się do wzmocnienia już istniejącego Jednolitego rynku cyfrowego, wykorzystując procesy cyfryzacji gospodarek jako bodziec stymulujący wzrost zarówno regionu, jak i całej UE.

WYOBRAŹ SOBIE EUROPĘ ŚRODKOWO-WSCHODNIĄ W 2035…

Przypadek Krakowa pokazał, że rewolucyjna transformacja miasta, oparta na technologii autonomicznych pojazdów, jest możliwa. Projekt został powielony w wielu miastach regionu. Zwiększone zapotrzebowanie na usługi big data processing sprawiło rozwinięcie się tzw. wysp danych w Czechach i na Słowacji do prawdziwych gigantów, którzy tworzą rozwiązania adaptowane na całym świecie. Wkrótce zautonomizowane zostały także międzynarodowe połączenia autobusowe, m.in. przy udziale polskich producentów autobusów, którzy mogli korzystać z prawdziwego skarbu wiedzy, jakim były pilotażowe projekty dotyczące autonomicznych pojazdów w całej EŚW. Dzięki przemyślanej implementacji technologii 5G przy rozwoju połączeń drogowych, autonomiczny pojazd może przejechać z Tallinna do Zagrzebia bez przerw w dostępie do sieci.

Bez tak dobrze rozwiniętej sieci połączeń, ośrodki e-handlu w centralnej Polsce oraz liczne mniejsze huby w EŚW nie mogłyby rozwinąć się do obecnej skali. Dzięki flocie jeżdżących i latających autonomicznych pojazdów pocztowych zbudowanej wspólnym wysiłkiem 12 krajów-sygnatariuszy Inicjatywy Cyfrowego Trójmorza, koszt i czas przesłania paczki między dowolnymi krajami regionu nie różni się od wysłania paczki krajowej. Trudno przecenić wpływ tej infrastruktury na boom w segmencie MŚP, który można obserwować w regionie od kilku lat.

Zaledwie dekadę temu cyberbezpieczeństwo było domeną powiązaną przede wszystkim z sektorem militarnym, finansowym i IT. Dziś potrzeba zwiększania cyberbezpieczeństwa rośnie również w innych obszarach. Atak sabotażowy na ukraińskie sieci elektroenergetyczne w 2016 r. udowodnił, jak znaczące

4 Szereg krajów, takich jak Estonia, rozważa obecnie taką opcję. Zobacz 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

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

konsekwencje takie ataki mogą mieć dla infrastruktury krytycznej. Szereg badań potwierdza, że sektor energetyczny i komunikacyjny/transportowy są szczególnie narażone na tego typu ataki:

- Według Instytutu Ponemon cyberprzestępczość w sektorze energetycznym i sektorze usług użyteczności publicznej generuje straty rzędu 12,8 mln USD rocznie;
- PwC donosi, że liczba ataków w sektorze energetycznym rośnie sześciokrotnie każdego roku;
- Każdego miesiąca przemysł lotniczy jest celem ponad 1 000 poważnych ataków cybernetycznych;
- Cisco informuje, że w 2016 r., liczba ataków na IoT wzrosła o 172 procent;
- Telefonica szacuje, że do 2020 r. 90 procent samochodów będzie podłączonych do sieci;
- Departament Bezpieczeństwa Krajowego USA ostrzega, że przeprowadzanie ataków na infrastrukturę krytyczną jest coraz tańsze i bezpieczniejsze (ze względu na problemy atrybucji), a ich konsekwencje dużo poważniejsze.

Wszystkie te ustalenia prowadzą do wniosku, że cyberbezpieczeństwo powinno być nie tylko elementem jednego z trzech filarów Trójmorza, a mianowicie filaru cyfrowego, ale również powinno stanowić część filaru energetycznego i transportowego.

CHINY W EŚW

Wiele państw Trójmorza łączy z Chinami bliska współpraca oraz liczne deklaracje chęci wzięcia udziału w Inicjatywie Pasa i Szlaku, którego jednym z elementów jest wymiar cyfrowy. Należy dokonać ostrożnej ewaluacji obszarów współpracy pod kątem skutecznego wykorzystania szans biznesowych, ale także odpowiedniego zabezpieczenia strategicznych interesów państw Trójmorza, NATO oraz UE.

W dokumencie Narodowej Komisji ds. Rozwoju i Reform ChRL z 2015 r.[6] wymienione są komponenty „Informacyjnego Jedwabnego Szlaku" (ang. Information Silk Road): budowa transgranicznych połączeń optycznych, światłowodowych połączeń podwodnych oraz realizacja projektów z zakresu komunikacji satelitarnej. Wyżej wymienione technologie zakładają duży zakres zależności wobec producenta, który ma kontrolę nad przepływem informacji oraz możliwość dostępu do jej zawartości. O ile w kontekście inicjatywy 16+1 działania Pekinu ograniczają się głównie do deklaracji, w krajach bliżej związanych z Chinami zrealizowano już pilotażowe projekty. Chiny zgodziły się udostępnić Pakistanowi na preferencyjnych warunkach nowoczesny system pozycjonowania satelitarnego BeiDou do celów wojskowych i cywilnych, który jest alternatywą dla amerykańskiego standardu GPS lub rosyjskiego systemu GLONASS[7]. Chiny zyskują więc narzędzie politycznego nacisku wobec partnera, co w świetle nuklearnego potencjału Pakistanu nabiera strategicznego wymiaru. Obecne jest tutaj charakterystyczne dla międzynarodowych działań Pekinu połączenie motywacji gospodarczych i politycznych.

Należy ostrożnie wyodrębnić obszary, gdzie zaangażowanie Chin w projekty Cyfrowego Trójmorza będzie wiązało się z obopólnymi korzyściami gospodarczymi i nie będzie generowało strategicznych zagrożeń bezpieczeństwa. Jednym z takich obszarów może być e-handel rozwijający się przy węzłach komunikacyjnych. Krokiem w kierunku materializacji takiej idei jest m.in. porozumienie podpisane w 2017 r. między Pocztą Polską a China Post dotyczące transportu przesyłek do Europy drogą lądową, które zakłada stworzenie dedykowanego węzła przeładunkowego.

Model współpracy oferowany w ramach 16+1 jest realizowany przez Chiny na całym świecie, głównie w krajach rozwijających się, które często mają większy kłopot z uzyskaniem dofinansowania projektów infrastrukturalnych niż członkowie UE. Inwestycje lub kredyty oferowane przez 16+1 często zawierają klauzule, które obligują kraj-klienta do realizacji projektu

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

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

przy użyciu kontrahentów z Chin, co znacząco ogranicza potencjał stymulacji gospodarki. Klauzula taka narusza prawo unijne, które wymaga przeprowadzenia otwartego przetargu na wykonawcę. Oferta Chin jest także mało konkurencyjna wobec alternatywnych form finansowania oferowanych w ramach UE, np. poprzez Europejski Bank Inwestycyjny[8]. Ze względu na powyższe, projekty realizowane dotychczas w ramach 16+1 skupiają się głównie w pięciu krajach nie należących do UE oraz dotyczą przede wszystkim infrastruktury transportowej i energetycznej.

Biorąc pod uwagę dynamikę odśrodkowych procesów zachodzących w UE, nie należy wykluczać intensywniejszych prób ugruntowania chińskiej pozycji w regionie. Subsydiowanie technologii o strategicznym znaczeniu lub otwarcie chińskiego rynku na import z krajów EŚW może stanowić atrakcyjną alternatywę dla utrzymania wzrostu gospodarczego w przypadku zmniejszenia dostępnych funduszy UE, szczególnie w perspektywie planowanego obniżenia poziomu funduszy strukturalnych po roku 2020. Beneficjentem tych funduszy w znacznej mierze są kraje, które wstąpiły do UE po 2004 r. Ewentualne dostosowanie warunków kredytowania do potrzeb unijnych członków formatu 16+1 może zwiększyć konkurencyjność oferty Pekinu.

Ewentualne większe zaangażowanie Chin w EŚW wiąże się z szeregiem wyzwań. Dotyczą one zarówno strategicznego charakteru technologii komunikacyjnych będących fundamentem bezpieczeństwa, jak również standardów realizacji projektów, cyberbezpieczeństwa systemów, poszanowania kwestii związanych z prywatnością i ochroną własności intelektualnej. Współpraca z Chinami w ramach rozwoju inicjatywy Cyfrowego Trójmorza z uwzględnieniem powyższych ograniczeń jest możliwa, ale wymaga odpowiedniego odniesienia się do wyżej wymienionych kwestii oraz identyfikacji obszarów współpracy korzystnej dla obu stron.

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

WYOBRAŹ SOBIE EUROPĘ ŚRODKOWO-WSCHODNIĄ W 2035…

Konstanca stała się regionalnym centrum prowadzenia działalności gospodarczej i atrakcyjnym miastem dla przedsiębiorców, jednym z najbardziej innowacyjnych w Rumunii i w EŚW. Globalne firmy ICT wraz z akademickimi laboratoriami innowacji otworzyły cyfrowe centra w Konstancy, mieście, które już w dużej mierze skorzystało na swoim ogromnym potencjale jako aktywnego miejsca inteligentnego rozwoju cyfrowego. Współpracując z lokalnymi i regionalnymi MŚP, globalni liderzy technologiczni szeroko wspierają start-upy oferując młodym przedsiębiorcom wspólną przestrzeń do współpracy, aby przyspieszyć rozwój ich firm i nowych umiejętności. Konstanca nawiązała partnerskie stosunki z wieloma miastami całej EŚW i jako dojrzała i kreatywna społeczność stała się wzorem do naśladowania jeśli chodzi o rozwój gospodarki i społeczeństwa cyfrowego.

CYBERBEZPIECZEŃSTWO NA AGENDZIE POLITYCZNEJ INICJATYWY TRÓJMORZA

Przez wiele lat państwa EŚW (z wyjątkiem Estonii) nie miały silnego głosu w dyskusji o cyberbezpieczeństwie, szczególnie w zakresie politycznych rozwiązań. Rok 2017 nie przyniósł oczekiwanych rezultatów związanych z decyzjami dotyczącymi cyberbezpieczeństwa w wymiarze międzynarodowym. Fiasko prac Grupy Ekspertów Rządowych ONZ (ang. UN Group of Governmental Experts) w latach 2016–2017 sprawiło, że społeczność międzynarodowa musi szukać innych przestrzeni do dyskusji na temat zastosowania prawa międzynarodowego do działań w cyberprzestrzeni, jak również rozwijania norm odpowiedzialnego zachowania.

Inicjatywa Trójmorza może wykorzystać szansę i wypełnić istniejącą lukę. Państwa regionu powinny aktywnie włączyć się do debaty związanej z cyberbezpieczeństwem, nadając jej nowy impuls poprzez swoje propozycje i działania. EŚW ma silny potencjał wpływu zarówno na kontynencie, jak i na świecie, a narażone na konflikty i napięcia w wymiarze cyfrowym kraje regionu mogą, a nawet powinny,

wnieść wiele w dyskusję dotyczącą działań budujących stabilność i większe zaufanie w tej domenie. Trójmorze powinno więc odgrywać istotną rolę w opracowywaniu polityk i strategicznych koncepcji związanych z cyberbezpieczeństwem, a także podejmować działania w standaryzacji procesów, technologii i rozwiązań. Rozmowę nad priorytetami należy podjąć z innymi partnerami, także z aktorami niepaństwowymi. Miejscem, które regularnie gości najważniejszych ekspertów i decydentów z tej dziedziny jest znajdujący się w sercu regionu Kraków i organizowane tutaj coroczne Europejskie Forum Cyberbezpieczeństwa – CYBERSEC.

W 2019 r. Słowacja obejmie przewodnictwo na forum OBWE, a Rumunia przejmie prezydencję w Radzie Unii Europejskiej. To doskonały czas, aby państwa Trójmorza ustaliły wspólną agendę w zakresie cyberbezpieczeństwa. Ważnym tematem do poruszenia powinna być implementacja i wzmacnianie środków budowy zaufania w cyberprzestrzeni (ang. Confidence Building Measures, CBM). Jedną z kwestii, które powinny zostać podjęte w ramach Inicjatywy Cyfrowego Trójmorza, jest poszerzenie spektrum działań Central European Cyber Security Platform (kraje V4 oraz Austria) tak, aby między innymi zwiększać cyberbezpieczeństwo infrastruktury krytycznej. Ważnym komponentem wspólnych działań powinna być współpraca między CERT-ami.

Państwa Cyfrowego Trójmorza powinny wspólnie wykorzystać swoje położenie na wschodniej flance Sojuszu, aby nadać ton aktywnościom wychodzącym naprzeciw zagrożeniom hybrydowym. Należy tego dokonać przede wszystkim w ramach projektu B9, którego format koncentruje się przede wszystkim na kwestiach bezpieczeństwa i obronności w regionie. Niemniej z uwagi na fakt, że wszyscy członkowie forum B9 uczestniczą w Inicjatywie Trójmorza, kwestie te są również do pewnego stopnia przedmiotem troski państw Trójmorza.

Wypracowanie wspólnej strategii, obejmującej współpracę wszystkich członków ma ogromne znaczenie. Uzasadnia to również fakt, że centra kompetencji NATO specjalizujące się w tej kwestii znajdują się w regionie EŚW: Centrum Eksperckie ds. Współpracy w Dziedzinie Cyberobronności (ang. Cooperative Cyber Defence Centre of Excellence) w Tallinnie, Centrum Eksperckie Kontrwywiadu NATO w Krakowie, Centrum Eksperckie ds. Komunikacji Strategicznej (ang. Strategic Communications Centre of Excellence) w Rydze czy Centrum Eksperckie Rozpoznania Osobowego (HUMINT) (ang. Human Intelligence Centre of Excellence) w Oradei. Wspólne działania Inicjatywy Trójmorza powinny wpisać się mocno w najnowsze postanowienia NATO i UE związane z cyberobroną, wspierając ich realizację jako koalicja państw, które łączą te same zagrożenia. Powinny opierać się na istniejącym *know-how,* wykorzystując jednocześnie własne rozwiązania technologiczne. Projekt powinien zostać zrealizowany w zakresie, który definiuje PESCO, czyli wzmacniać zdolności cyberobrony poprzez współpracę przede wszystkim w trzech obszarach: dzielenia się informacjami, wspólnych ćwiczeń i wsparcia operacyjnego. Wykaz projektów PESCO zawiera dwie inicjatywy dotyczące cyberobronności: ustanowienie Platformy wymiany informacji na temat zagrożeń dla cyberbezpieczeństwa i reagowania na incydenty cybernetyczne (ang. Cyber Threats and Incident Response Information Sharing Platform) oraz powołanie Zespołów szybkiego reagowania na zagrożenia cybernetyczne i wzajemnej pomocy w zakresie cyberbezpieczeństwa (ang. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security). Państwa Trójmorza powinny się w nie zaangażować przynajmniej w charakterze obserwatorów.

Wspólny wysiłek członków Inicjatywy Cyfrowego Trójmorza mający na celu wzmacnianie cyberbezpieczeństwa regionu powinien obejmować także inicjatywy związane z edukacją, wymianą ekspertów, szkoleniami, ćwiczeniami, itp. Państwa EŚW w wielu przypadkach posiadają specyficzne doświadczenia związane z cyberbezpieczeństwem (np. zagrożenia hybrydowe z akcentem wielowymiarowych działań cyfrowych), w ramach których mogą podjąć działania wzmacniające kompetencje całej społeczności międzynarodowej.

Narzędzia cyfrowe w sposób znaczący wzmacniają siłę i możliwości oddziaływania na publiczność. Wpływając na postrzeganie można kształtować ludzkie emocje, opinie, a w konsekwencji – decyzje i działania. W dobie wszechobecnych narzędzi cyfrowych manipulowanie obrazem, dźwiękiem czy nagraniami wideo jest bardzo łatwe. Biorąc pod uwagę wysoki potencjał *viralowy* takich treści, wykorzystanie *fake news* może być bardzo skuteczną metodą prowadzenia wojny informacyjnej.

W ten sposób wojna informacyjna w cyberprzestrzeni może stać się bardzo atrakcyjnym narzędziem prowadzenia konfliktów hybrydowych. Pojęcia takie jak *fake news* czy dezinformacja to żadna nowość. Mimo powszechnego przekonania, to nie USA, ale kraje regionu EŚW (zwłaszcza Ukraina i Polska), były pierwszymi, które doświadczyły konsekwencji wojny informacyjnej.

Wraz z East StratCom Task Force (EEAS) i Centrum Eksperckim ds. Komunikacji Strategicznej (Strategic Communications Centre of Excellence) kraje skupione wokół Inicjatywy Cyfrowego Trójmorza powinny zaangażować się w zwalczanie kampanii dezinformacyjnych poprzez stworzenie platformy wymiany doświadczeń w walce z dezinformacją i ustanowienie funduszu na rzecz wspierania rozwoju wiedzy eksperckiej, prowadzenia analiz i publikacji materiałów tłumaczonych z języków narodowych państw Trójmorza na język angielski.

PODSUMOWANIE

INICJATYWA CYFROWEGO TRÓJMORZA: BUDOWANIE WSPÓŁPRACY W WYMIARZE CYFROWYM W EUROPIE ŚRODKOWO-WSCHODNIEJ

EŚW nabiera kluczowego znaczenia w geopolitycznej rywalizacji pomiędzy Chinami a Stanami Zjednoczonymi.

Dynamiczna transformacja cyfrowa gospodarek EŚW, coraz bardziej znaczący udział cyberprzestrzeni w relacjach międzynarodowych oraz nowe transgraniczne zagrożenia bezpieczeństwa o charakterze hybrydowym wymagają nadania Inicjatywie Trójmorza silnego wymiaru cyfrowego, którego nieodzownym elementem jest komponent cyberbezpieczeństwa.

Cyberprzestrzeń cechuje „plastyczność", dzięki czemu można ją ukształtować w sposób, który może zwiększyć znaczenie geostrategiczne i geoekonomiczne regionu EŚW i zapewnić wzrost gospodarczy i rozwój e-społeczeństwa bazujące na rynku cyfrowym (swobodnym przepływie danych, e-handlu itd.).

Poprzez pogłębienie współpracy państw regionu, wzmocniona zostanie także spójność UE i całej wspólnoty transatlantyckiej. Pogłębiona zostanie także strategiczna obecność Stanów Zjednoczonych w Europie.

Silna współpraca regionalna we wszystkich kwestiach dotyczących cyberbezpieczeństwa, w tym bezpieczeństwa energetycznego, jest warunkiem przyszłego wzrostu gospodarczego („usieciowionej" gospodarki cyfrowej) oraz bezpieczeństwa (wspólne cyberzagrożenia, w tym dezinformacja) w EŚW.

CEL INICJATYWY:

Trójmorze to 12 krajów UE, 114 milionów obywateli zamieszkujących ponad 28 procent terytorium UE i wytwarzających PKB na poziomie 1,6 bilionów dolarów. Nieustannie zmieniająca się globalna architektura bezpieczeństwa sprawia, że region EŚW odgrywa coraz większe znaczenie dla aktorów takich jak USA, Wielka Brytania, Chiny czy Rosja. Poszerzenie Inicjatywy Trójmorza o wymiar cyfrowy i cyberbezpieczeństwo, obok już istniejących filarów transportowego i energetycznego, może mieć geopolityczne i geoekonomiczne konsekwencje wykraczające daleko poza granice EŚW. Kluczowymi obszarami Inicjatywy Cyfrowego Trójmorza są rozwój infrastruktury cyfrowej w dobie technologii 5G, wspólne inwestycje w supernowoczesne technologie takie jak Internet rzeczy, blockchain i sztuczna inteligencja oraz strategiczna i taktyczna współpraca w zakresie zwalczania cyberzagrożeń i dezinformacji.

PARNTERZY INICJATYWY:

GLOBSEC to globalny think tank zaangażowany w zwiększenie bezpieczeństwa, dobrobytu i zrównoważonego rozwoju w Europie i na świecie. Jego misją jest wpływanie na przyszłość poprzez generowanie nowych pomysłów i rozwiązań dla lepszego i bezpieczniejszego świata. W świecie wzajemnych powiązań, GLOBSEC stymuluje dialog publiczno-prywatny kształtujący plany działania na przyszłość. Mając globalne ambicje i czerpiąc ze swoich środkowoeuropejskich korzeni GLOBSEC pragnie wnieść swój wkład do programów o kluczowym znaczeniu dla Europy. GLOBSEC działa w duchu wartości europejskich i współpracy międzynarodowej. Coroczne Forum GLOBSEC w Bratysławie, jedna z wiodących konferencji dotyczących globalnego bezpieczeństwa na świecie, przybliża GLOBSEC do realizacji tego celu.

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

Instytut Rozwoju i Stosunków Międzynarodowych (IRMO) to publiczny, naukowy ośrodek badań politycznych o charakterze non-profit, zaangażowany w studia interdyscyplinarne dotyczące europejskich i międzynarodowych stosunków gospodarczych, politycznych, kulturowych i komunikacyjnych. Założony w 1963 roku przez Uniwersytet w Zagrzebiu i chorwacką Izbę Handlową pod nazwą Instytutu Badawczego Afryki (ang. Africa Research Institute), Instytut zmieniał swoją nazwę kilkukrotnie, odzwierciedlając tym samym zmiany w kręgu swoich zainteresowań naukowych. Podstawową misją Instytutu jest rozwijanie i rozpowszechnianie teoretycznej, metodologicznej i technicznej wiedzy oraz umiejętności niezbędnych do naukowej i profesjonalnej interpretacji i oceny współczesnych stosunków międzynarodowych wpływających na różne ludzkie działania i pokrewne trendy rozwojowe istotne z punktu widzenia Republiki Chorwacji. Tendencje rozwojowe są postrzegane w lokalnym, regionalnym, europejskim i globalnym kontekście. Instytut zatrudnia 44 pracowników, spośród których 16 to członkowie kadry akademickiej.

New Strategy Center to rumuński think tank specjalizujący się w problematyce dotyczącej polityki zagranicznej, obronności i bezpieczeństwa. Jest to pozarządowa i bezpartyjna organizacja o charakterze non-profit, która finansuje swoją działalność ze środków własnych. Działania NSC skupiają się wokół trzech głównych obszarów: opracowywania analiz i ekspertyz dla decydentów, organizowania regularnych, wewnętrznych i publicznych debat na aktualne tematy, oraz poszerzenie zasięgu swojej działalności poprzez partnerstwa z podobnymi instytucjami i organizacjami w Europie i Stanach Zjednoczonych, oraz wspólne przygotowywanie dokumentów programowych i udział w międzynarodowych konferencjach. Priorytetowymi obszarami zainteresowania NSC pod kątem bezpieczeństwa i pojawiających się możliwości współpracy dwustronnej i wielostronnej są basen Morza Czarnego i obszar Bałkanów w bliskim sąsiedztwie Rumunii. Obecne działania NSC obejmują również takie kwestie jak wewnętrzny postęp w dziedzinach istotnych z punktu widzenia bezpieczeństwa narodowego Rumunii, zamówienia publiczne związane z modernizacją armii i obronnością, bezpieczeństwo energetyczne i nadzieje związane z nowymi technologiami oraz zagrożenia niekonwencjonalne i hybrydowe, w tym cyberprzestrzeń i dyplomacja publiczna.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (Think Tank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.

Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa CYBERSEC oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.

Instytut Kościuszki jest wydawcą European Cybersecurity Journal (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.

Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24, www.ik.org.pl, e-mail: instytut@ik.org.pl

PARTNERZY INICJATYWY CYFROWEGO TRÓJMORZA:

GLOBSEC
IDEAS SHAPING THE WORLD

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

NEW STRATEGY CENTER

TWÓRCA INICJATYWY CYFROWEGO TRÓJMORZA:

INSTYTUT KOŚCIUSZKI