Bezpieczne cyfrowe DNA

REGIONU TRÓJMORZA

IZABELA ALBRYCHT, WIOLETTA BRZĘCKA, FAUSTINE FELICI,
AGNIESZKA KONKEL, KAMIL MIKULSKI, ROBERT SIUDAK, JOANNA ŚWIĄTKOWSKA

INSTYTUT KOŚCIUSZKI

Bezpieczne cyfrowe DNA
REGIONU TRÓJMORZA

AUTORZY: IZABELA ALBRYCHT, WIOLETTA BRZĘCKA,
FAUSTINE FELICI, AGNIESZKA KONKEL, KAMIL MIKULSKI,
ROBERT SIUDAK, JOANNA ŚWIĄTKOWSKA

INSTYTUT KOŚCIUSZKI

AUTORZY:

INSTYTUT KOŚCIUSZKI

Izabela Albrycht
Redakcja merytoryczna

Wioletta Brzęcka
Społeczne uwarunkowania poziomu cyberbezpieczeństwa państw Trójmorza

Faustine Felici
Rozwój cyberbezpieczeństwa w regionie Trójmorza z perspektywy prawnej
Region Trójmorza w kontekście ekologicznym i środowiskowym

Agnieszka Konkel
Analiza PESTLE – podsumowanie

Kamil Mikulski
Perspektywy gospodarcze regionu Trójmorza
Rozwój technologiczny w regionie Trójmorza

Robert Siudak
Innowacje cyfrowe w regionie Trójmorza

Dr Joanna Świątkowska
Geopolityczny krajobraz cyberzagrożeń w regionie Europy Środkowo-Wschodniej

TŁUMACZENIE: Adam Ladziński, KOORDYNACJA: Kamil Mikulski, PROJEKT I SKŁAD: Joanna Świerad-Solińska

Opracowanie tego raportu było możliwe dzięki wsparciu Google.

Podziękowania: Konrad Kas (Google), Ewa Lis-Jeżak (IDC)

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki
ul. Feldmana 4/9-10
31-130 Kraków, Polska
+48 12 632 97 24
www.ik.org.pl
instytut@ik.org.pl

SPIS TREŚCI

STRESZCZENIE

Biologiczne DNA określa podstawowe cechy istot żywych, nadając niejako światu organicznemu jego niepowtarzalne własności. Tworząc obecnie nowy cyfrowy świat, możemy odwołać się do tych fundamentalnych kwestii, starając się ukształtować jego esencję, uczynić go bezpiecznym, odpornym i zdolnym do prężnego rozwoju teraz i w przyszłości. Digitalizacja to nieodzowny proces przenikający każdy aspekt naszej rzeczywistości – od spraw codziennych po gospodarki, państwa i społeczeństwa. Wbudowanie bezpieczeństwa w to zjawisko oraz w bardziej szczegółowe rozwiązania ma zatem kluczowe znaczenie pod względem zarówno funkcjonowania, jak i dobrobytu społeczeństwa. Jeśli myślimy o wdrażaniu nowych technologii cyfrowych, wprowadzaniu infrastruktury cyfrowej lub tworzeniu cyberproduktów i usług oraz konstruowaniu rozstrzygnięć, regulacji i standardów – winniśmy je projektować w odniesieniu do tego DNA, w całym cyklu życia tych zjawisk biorąc pod uwagę cyberbezpieczeństwo, które powinno być domyślnie wbudowane w cyfrowe DNA osób i społeczeństw.

W obliczu przyszłego rozwoju takich technologii jak sztuczna inteligencja, informatyka kwantowa, Internet Rzeczy czy blockchain oraz wobec ich mariaży podejście nietracące z oczu DNA może służyć rozpoznaniu rodzajów przyszłego ryzyka i przeciwdziałaniu im zawczasu, tak aby sfera cyfrowa nie ulegała osłabieniu. Duża szybkość digitalizacji doprowadzi w nieodległej perspektywie do poważnych wyzwań. Dla bezpieczeństwa cyfrowego DNA świata musimy wprowadzać innowacje stające naprzeciw zagrożeniom nowego typu. Ale co najważniejsze, musimy współpracować, angażując rozmaite zainteresowane strony. Bezpieczeństwo cyfrowego DNA świata to odpowiedzialność wszystkich interesariuszy. Wymaga dzielenia się informacjami, wzmacniania współpracy w obrębie sektora publicznego, prywatnego, naukowego i społeczeństwa obywatelskiego, jak również pomiędzy nimi, a także tworzenia inkluzywnych platform współpracy. Wysiłki w gronie państw sojuszniczych mają zasadnicze znaczenie we wspieraniu przyjęcia omawianych zasad w aparatach państwowych i procesach decyzyjnych na szczeblu międzynarodowym. Dla zachowania wolnej, otwartej i pokojowej cyberprzestrzeni w nadchodzących latach oraz utrzymania pozytywnej koniunktury i tempa wzrostu gospodarczego na świecie.

Region Trójmorza – obszar jednego z najszybciej rozwijających się ekosystemów cyfrowych w Europie – wykazuje duży potencjał wzrostu w dobie gospodarki opartej na danych. To również znakomite miejsce na przyspieszenie procesu wzmacniania cyberbezpieczeństwa w cyfrowym DNA globu. Wielu problemom i wyzwaniom w tej dziedzinie region może zaradzić samodzielnie i na własnych zasadach, dbając zarazem, by działać w duchu i komplementarnie do szerszego wymiaru integracji w obrębie Unii Europejskiej oraz wspólnoty transatlantyckiej.

Transformacja cyfrowa z wpisanym w nią komponentem cyberbezpieczeństwa może zbudować przewagi komparatywne regionu oraz przyczynić się do przyspieszonego wzrostu gospodarczego w czasach pogłębiającej się konwergencji między światem fizycznym a cyfrowym (ang. *physical and digital convergence*). Jednak możemy się również spodziewać, że wraz z tym procesem skala i zaawansowanie ataków cyfrowych będzie wzrastać, co w średnim okresie zwiększy straty z tytułu ataków cyfrowych i narazi gospodarki całego świata, w tym Trójmorza (3S), na znaczne szkody. Zagrożenia te dotyczą sektorów kluczowych dla dalszego rozwoju i skomunikowania Trójmorza – transportowego, energetycznego i cyfrowego.

Ponadto pod koniec drugiej dekady XXI wieku dotarliśmy do momentu, w którym Europa Środkowo-Wschodnia (EŚW) zaczęła w sposób szczególny odczuwać geopolityczny wiatr zmian. Jego źródłami są napawająca obawami strategiczna i wielowymiarowa rywalizacja Stanów Zjednoczonych i Chińskiej Republiki Ludowej, podejmowanie przez Rosję agresywnych działań w regionie, a także wewnątrzkontynentalna

dynamika procesu dezintegrującego unijny konstrukt polityczny, czego symbolem stał się Brexit. To rzecz jasna uproszczona lista symptomów i sygnałów świadczących o zbliżających się zmianach. Obecna sytuacja przywodzi na myśli przemowę premiera Wielkiej Brytanii Harolda Macmillana z 1960 roku (choć wygłoszoną w innym historycznie i geograficznie kontekście): *The wind of change is blowing through this continent*.

Aktualnie obserwowane zmiany stawiają region Trójmorza w wyjątkowym położeniu, przez które „wiatr" ten z pewnością będzie odczuwalny z jeszcze większą niż obecnie siłą. Dlatego teraz szczególnie istotne jest aktywizowanie potencjału bezpiecznej cyfrowej transformacji gospodarek krajów Trójmorza do wzmocnienia polityczno-ekonomicznie całego kontynentu, ale także dalszego rozwoju partnerskich strategicznych relacji transatlantyckich.

Technologiczny wyścig, do którego jako Europa Środkowo-Wschodnia musimy nie tylko stanąć, ale także mieć odpowiednie zasoby, aby w nim uczestniczyć jak równy z równym, na dobre się rozpoczął. Wykładniczy rozwój technologii cyfrowych poszerza pole gry i mocno komplikuje ocenę potencjałów i siły państw. Za sprzyjające uznać można strategiczne cele polityk unijnych nakierowane na budowanie cyfrowej suwerenności wspólnoty czy też pod pewnymi względami uwarunkowania geoekonomiczne, takie jak rozrywanie (*decoupling*) globalnego łańcucha wartości w sektorze nowoczesnych technologii cyfrowych i spodziewane zmniejszenie atrakcyjności inwestycyjnej CHRL (pod warunkiem że na dłuższą metę nie doprowadzi to do zbyt głębokich zawirowań gospodarczych na świecie). Mocniejsze włączanie się Stanów Zjednoczonych w relacje dwustronne i regionalne z EŚW w zakresie cyberbezpieczeństwa i ucyfrowienia tworzy w regionie potencjał synergii. Współpracę Trójmorza z USA należy, skupiając się na transferze technologii, wymianie doświadczeń i osiągnięć w przemianach cyfrowych oraz sposobach reagowania na cyberzagrożenia, właściwie zorganizować i realizować.

Przeprowadzona w raporcie analiza PESTLE wskazuje z jednej strony na wyjątkową ekspozycję Trójmorza na zagrożenia hybrydowe, w tym cyfrowe, a także zawirowania polityczne i zmiany geopolityczne, a z drugiej na potencjał, jaki tkwi w jego gospodarce i społeczeństwie, który wraz ze wsparciem dla widocznych już pozytywnych tendencji rozwojowych może być wykorzystany do realizacji polityki dalszego bezpiecznego wzrostu gospodarczego w dobie nowego cyfrowego świata. Podejmując decyzję o nadaniu rozwojowi sektora cyberbezpieczeństwa wysokiego priorytetu, kraje regionu powinny zwrócić uwagę na szereg czynników i uwarunkowań natury politycznej, społeczno-ekonomicznej, technologicznej oraz prawnej i środowiskowej.

GŁÓWNE REKOMENDACJE

UWARUNKOWANIA POLITYCZNE

- W czasach przemodelowania światowego porządku i rosnącego znaczenia cyfrowych technologii w projekcji siły kraje regionu EŚW, z uwagi na swoje znaczenie geopolityczne, muszą jak najszybciej rozwinąć cyfrowe narzędzia defensywne i ofensywne, aby chronić bezpieczeństwo narodowe i realizować strategiczne interesy gospodarcze i polityczne.
- Region EŚW musi zaplanować systemowe działania, aby zbudować odporność na zagrożenia hybrydowe. W tym odpowiedzi na zagrożenia związane z walką informacyjną i dezinformacją, które skutkować mogą napięciami politycznymi, polaryzacją społeczeństwa i obniżaniem zaufania do władzy, a w rezultacie stanowić zagrożenie dla demokracji w regionie.
- Kraje Trójmorza (3S) muszą strategicznie przemyśleć swoją orientację względem ekonomicznej i cyfrowej ekspansji CHRL, realizowanej w formie Inicjatywy Pasa i Szlaku oraz Cyfrowego Jedwabnego Szlaku. Biorąc pod uwagę różnorakie współzależności między krajami oraz transgraniczny charakter tych projektów, konieczne jest wypracowanie wspólnego stanowiska w tak istotnych kwestiach jak np. bezpieczny model rozwoju sieci 5G.
- W kontekście sieci 5G kraje 3S – obok współpracy bilateralnej w regionie, której przykładem może być porozumienie rządów Rumunii i Polski, lub multilateralnej takiej jak Propozycje praskie na temat ustanawiania standardów bezpieczeństwa dla sieci 5G, w tym dostawców komponentów do jej budowy – powinny także zintensyfikować swoje zaangażowanie w prace Komisji Europejskiej nad zestawem narzędzi do zarządzania ryzykiem oraz niezbędnymi wymaganiami bezpieczeństwa 5G. Sieć piątej generacji będzie bowiem kluczowa dla dalszego rozwoju technologicznego i gospodarczego oraz bezpieczeństwa narodowego regionu.

UWARUNKOWANIA SPOŁECZNE

- Choć wielką przewagą komparatywną regionu 3S jest aktualnie dostępność wysoko wykwalifikowanych pracowników z wykształceniem w przedmiotach STEM, co w wielu państwach wynika z bogatej tradycji w zakresie nauk ścisłych i matematyki, to jednak należy systemowo odnieść się do problemu ograniczonej ich podaży względem rosnącego popytu.
- Należy łagodzić zagrożenia związane ze zjawiskiem starzenia się społeczeństwa, co może negatywnie wpłynąć na innowacyjny potencjał gospodarki. Region musi uniknąć dwóch zagrożeń, czyli sytuacji, w której kraje staną w obliczu wysokiego wzrostu gospodarczego, ale zmniejszającego się kapitału społecznego, rosnąć bowiem będzie grupa bardziej zależnych ekonomicznie osób starszych i jednocześnie maleć liczba efektywnych i innowacyjnych młodszych; proces ten może pogłębić istniejące już problemy strukturalne niedoinwestowania B+R w regionie EŚW.
- Należy do tych nowych długoterminowych cyfrowych wyzwań oraz potrzeb rynku dostosować systemy edukacji, które powinny odzwierciedlać obawy dotyczące zastąpienia licznych rzesz pracowników w ramach automatyzacji cyfrowej, robotyzacji i użycia sztucznej inteligencji, jak również tworzone przez postęp techniczny szanse na powstanie zupełnie nowych stanowisk, a także powinny uwzględniać interdyscyplinarną naturę świata rozszerzonego o wymiar cyfrowy.
- Warto badać, jak szkolnictwo wyższe Trójmorza – segment kluczowy w rozwoju potencjału gospodarki i innowacyjności oraz procesach ucyfrowienia – odpowiada na kwestię niedoboru kadr w ICT i STEM oraz jak wyglądają relacje między liczbą absolwentów tych kierunków a liczbą specjalistów z innych dziedzin. Również płeć warto postrzegać jako istotny element poszerzania rynku pracy w informatyce przez kształcenie w tej dziedzinie zrównoważonych płciowo kadr.
- Sektor cyberbezpieczeństwa powinien stać się jednym z priorytetowych obszarów naukowo-badawczych i edukacyjnych. Konieczne jest wsparcie ośrodków akademickich będących zapleczem kadrowym dla szeroko rozumianego sektora cyberbezpieczeństwa. Decydenci muszą mieć tego świadomość i jak najszybciej zwiększyć nakłady na naukę w tym obszarze oraz zaaplikować rozwiązania dostosowujące ofertę edukacyjną także do wyzwań związanych z potrzebą zapewnienia cyberbezpieczeństwa państwa i instytucji publicznych oraz biznesu.
- Cyberbezpieczeństwo regionu zależy również od umiejętności cyfrowych i świadomości cyfrowych zagrożeń po stronie użytkowników sieci i systemów ICT, dlatego państwa 3S powinny także rozwijać wiedzę i kompetencje w tym zakresie w ramach społeczeństwa. Należy zwrócić także uwagę na potrzebę edukacji społecznej dotyczącej skłonności do korzystania z cyfrowych rozwiązań oraz usług publicznych i komercyjnych.
- Działalność uczelni wyższych i wsparcie władz, w postaci utrzymania klimatu inwestycyjnego korzystnego dla angażowania kapitału oraz zapewnienia rozwiniętej infrastruktury cyfrowej, może sprawić, że region 3S będzie idealnym miejscem do zakładania centrów badań i rozwoju, Security Operations Centers (SOC) czy centrów usług chmurowych. Wiele z tych inwestycji już ma miejsce, ale z uwagi na zmiany geoekonomiczne, tj. rozrywanie łańcucha dostaw w sektorze ICT (*decoupling of global ICT supply chain*), proces ten można zintensyfikować.

UWARUNKOWANIA EKONOMICZNE

- W ramach realizacji celów rozwojowych kraje 3S powinny położyć nacisk na wsparcie swoich sektorów ICT, a szczególnie branży cyberbezpieczeństwa. Szanse ku temu są olbrzymie i wynikają m.in. z przewidywań odnośnie do wzrostu rynku cyberbezpieczeństwa globalnie, a także wzrostu PKB regionu (sięgającego 1,7 bln euro w roku 2017 i prognozowanego na 2,3 bln w 2030).

- Wykorzystując środki z funduszy unijnych, ale także publiczne środki krajowe i prywatne inwestycje, kraje 3S powinny strategicznie zaprojektować bezpieczną transformację cyfrową. Powinna uwzględnić budowę bezpiecznej infrastruktury telekomunikacyjnej piątej (i kolejnych) generacji, centrów przetwarzania danych i usług chmurowych, centrów innowacji cyfrowych (*digital innovation hubs*) czy centrów kompetencji (*centres of excellence*). Same inwestycje infrastrukturalne o znaczeniu transnarodowym mogą wymagać do roku 2030 270 mld euro. Zbiorczy popyt na szeroko rozumiane inwestycje w infrastrukturę wyniesie w całym regionie do roku 2030 nawet ok. 1,15 bln euro; nakłady na drogi, koleje, wodne drogi śródlądowe, porty, lotniska, linie energetyczne i telekomunikacyjne, cyfryzację – nawet ok. 530 mld euro.
- Finalizacja projektów infrastrukturalnych w ramach inicjatywy Trójmorza jest nie tylko istotna z punktu widzenia rozwoju gospodarczego regionu, ale także jego bezpieczeństwa. Polityka wsparcia dla rozwoju sektora cyberbezpieczeństwa ma znaczenie nie tylko z uwagi na potrzebę budowania krajowych zdolności zabezpieczenia kluczowych systemów infrastruktury, ale także z uwagi na spodziewane bezpośrednie i pośrednie korzyści ekonomiczne.
- Istnieje bezpośrednia współzależność pomiędzy bezpieczeństwem energetycznym a cyberbezpieczeństwem sektora energetycznego. Z tego względu polityka krajów regionu, zarówno w relacjach bilateralnych, jak i multilateralnych, powinna zostać odpowiednio dostosowana, tak aby uwzględnić kluczowy i transformujący sektor energetyczny wymiar cyfrowy. To samo tyczy się rozwijanych w ramach Trójmorza projektów transportowych (m.in. Via Carpatia) i cyfrowych (np. planowana Cyfrowa Autostrada Trójmorza). Innymi słowy, wszystkie planowane w ramach 3SI elementy infrastruktury w czasie budowy i utrzymania wymagają implementacji zaawansowanych systemów ICT i cyberbezpieczeństwa. Jest to wielka szansa dla rozwoju rodzimego rynku tych produktów i usług.
- Przed zbliżającym się kolejnym szczytem 3SI w Estonii należy zwrócić uwagę na potrzebę znacznego przyspieszenia w zakresie operacjonalizacji koncepcji infrastrukturalnych projektów cyfrowych zawartych na liście projektów priorytetowych przyjętej przez szczyt budapeszteński w 2018 r. Ich stopień zaawansowania w stosunku do dwóch pozostałych grup projektów – transportowych i energetycznych – jest najmniejszy, jednocześnie należy nadać części z nich status programu flagowego porównywalny z inicjatywami międzynarodowymi budującymi klasyczną infrastrukturę transportową, takimi jak trasa międzynarodowa Saloniki–Kłajpeda (Via Carpatia), korytarz bałtycko-adriatycki czy droga ekspresowa Tallin–Warszawa (Via Baltica).

UWARUNKOWANIA TECHNOLOGICZNE

- Współpraca krajów 3SI oprócz wymiaru infrastrukturalnego powinna także objąć szereg miękkich inicjatyw współpracy w obszarze cyberbezpieczeństwa oraz budowania i zwiększania zdolności w zakresie innowacji cyfrowych. Wiele z nich zostało przedstawionych w ramach inicjatywy Cyfrowego Trójmorza (Digital 3 Seas) opracowanej w partnerstwie z think tankami regionu w 2018 roku[1].
- Region 3S powinien jeszcze bardziej zwiększyć dynamikę rozwoju innowacji w zakresie technologii istotnych z punktu widzenia zmian krajobrazu bezpieczeństwa cyfrowego – sztuczna inteligencja, 5G, blockchain, technologie kwantowe, Internet Rzeczy – a jednocześnie w różnych sektorach gospodarki i instytucjach publicznych w poszczególnych krajach powinny być stale realizowane ich pilotażowe wdrożenia.
- Dostrzegalne są zalążki specjalizacji technologicznej w ramach krajów 3S. Należy potraktować to jako dobry punkt wyjścia do wymiany doświadczeń i dobrych praktyk w zakresie regulacji i aplikacji technologii w regionie w ramach współpracy bilateralnej oraz multilateralnej.

1 Digital 3 Seas, [online]: https://digital3seas.eu.

Taka kooperacja jest racjonalna i efektywna, biorąc pod uwagę ograniczone zasoby ludzkie, innowacyjne i naukowo-badawcze 3S przy jednocześnie galopującym globalnym rozwoju technologicznym, który w perspektywie średniookresowej może zostawić te kraje daleko w tyle za liderami innowacji technologicznych.

- W ramach nowej wieloletniej perspektywy finansowej UE kraje 3S powinny w sposób skoordynowany lobbować za alokacją środków, które zwiększą ich innowacyjny potencjał technologiczny (infrastruktura cyfrowa, B+R, edukacja), pogłębią specjalizację technologiczną (programy badawcze, wsparcie dla startupów, centra innowacji cyfrowych, centra kompetencji, inicjatywy kooperacyjne) oraz przyspieszą wdrożenia technologii cyfrowych w przemyśle, MŚP czy instytucjach publicznych. Należy zwrócić uwagę na wszystkie fazy zarówno badań i rozwoju, jak i realnego zastosowania technologii, gdyż tylko pełna sekwencja działań wygeneruje gospodarczą wartość dodaną w dłuższym okresie.

UWARUNKOWANIA PRAWNE

- Kraje 3S powinny podwyższać swój poziom cyberbezpieczeństwa i budować w tym zakresie zdolności poprzez ambitną, przemyślaną i świadomą silnej ekspozycji na zagrożenia hybrydowe i cyfrowe implementację ram prawnych proponowanych przez UE oraz strategicznych kierunków EU Digital Single Market. W tym przede wszystkim istotne jest wprowadzenie w życie opublikowanego w czerwcu 2019 r. aktu o cyberbezpieczeństwie (ang. Cybersecurity Act), czyli Rozporządzenia Parlamentu Europejskiego i Rady w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych.

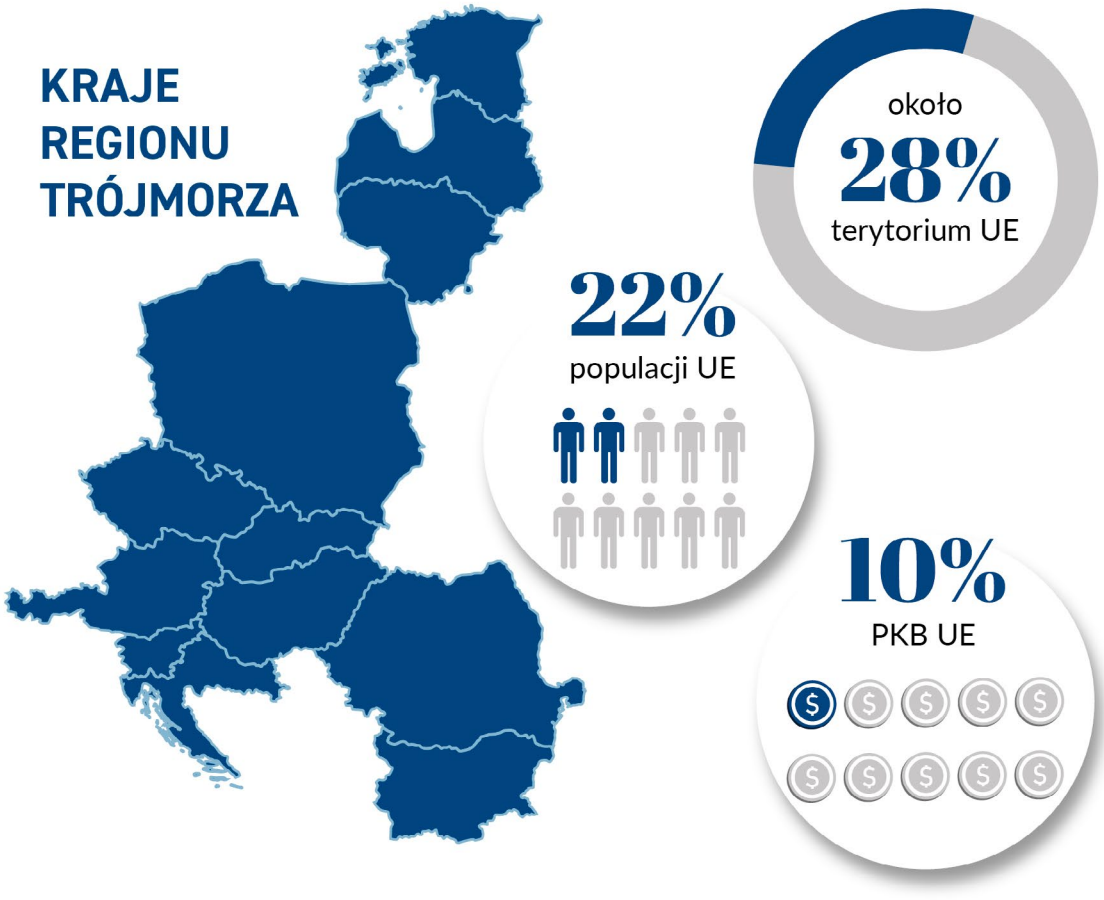
- Przykładem dobrego podejścia do kwestii regulacyjnych jest implementacja przez kraje 3S dyrektywy NIS, którą objęły one większą liczbę sektorów gospodarki niż przewidziano obligatoryjnie w dyrektywie.

- Wdrażając unijne regulacje, ale także kształtując i rozwijając otoczenie instytucjonalno-prawne dla cyberbezpieczeństwa, kraje Trójmorza muszą mieć na uwadze silną korelację między cyberzagrożeniami a położeniem geopolitycznym, a także potrzebę stworzenia konkurencyjnego otoczenia prawnego dla producentów i usługodawców w sektorze cyberbezpieczeństwa. Dotyczy to zwłaszcza procesu certyfikacji cyberbezpieczeństwa produktów czy usług i procesów dotyczących sieci i systemów informatycznych, gdyż rozwiązania te z pewnością wpłyną na konkurencyjność rozwiązań lokalnych producentów z branży cyberbezpieczeństwa.

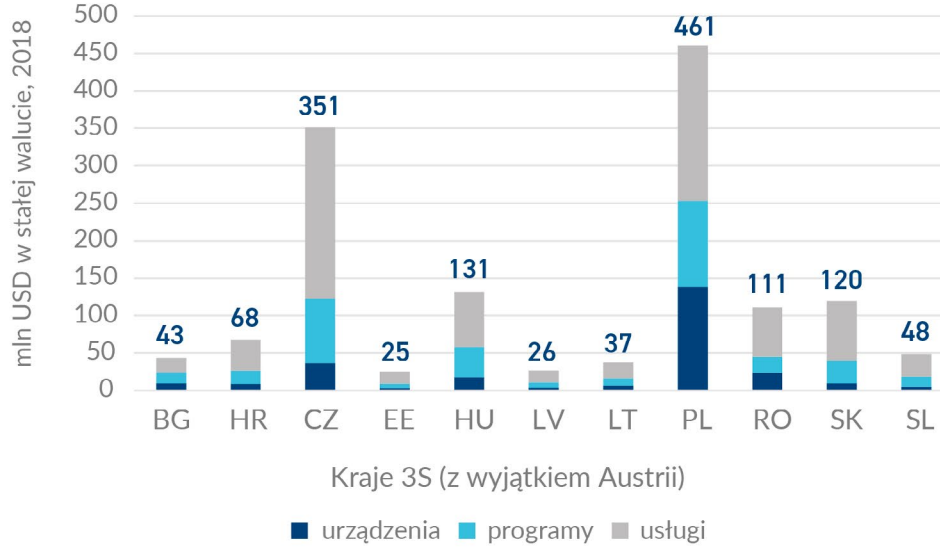
UWARUNKOWANIA ŚRODOWISKOWE

- Trójmorze z powodu produkcji i zużycia energii, które cechują się znacznym udziałem paliw kopalnych, a także spodziewanego szybkiego wzrostu branży ICT powinno dokładać starań i podejmować kroki, by zmierzać w stronę energetyki ekologicznej. Zużycie energii przez centra danych oraz sieci telekomunikacyjne wzrośnie w obecnej dekadzie odpowiednio o 35 oraz 150%, głównie przez intensywne wykorzystanie mobilnych usług internetowych oraz sprawniejsze i dające większe możliwości sieci komórkowe. Zgodnie z przewidywaniami sam rynek centrów danych odnotuje w latach 2018–2024 średnią roczną stopę wzrostu na poziomie 5%. Łatwo zatem zrozumieć, że skutki rozrostu tego sektora są potencjalnie groźne dla przyrody, jeśli nie będą go zasilały bezemisyjne źródła energii.

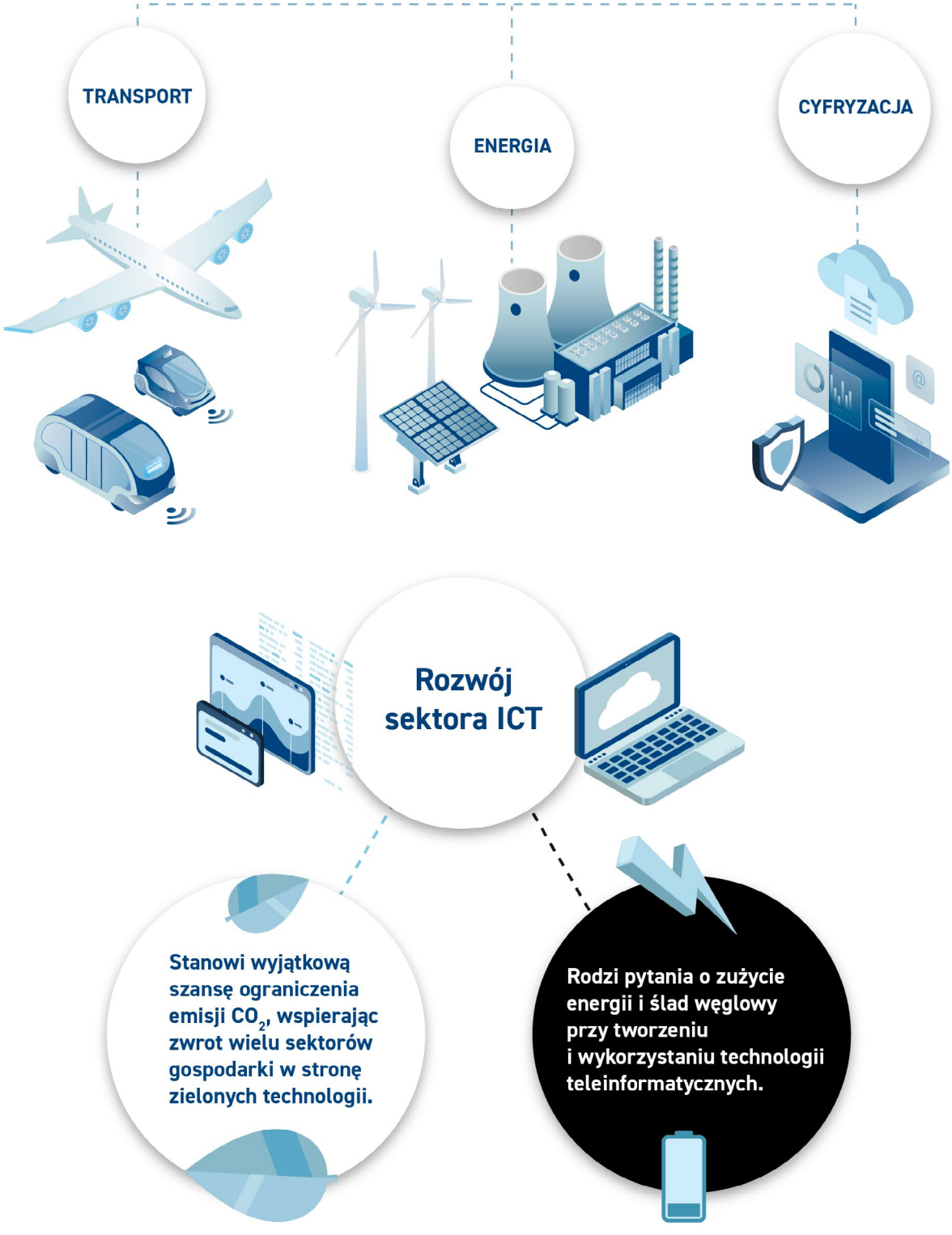
- Czerpanie energii z czystych źródeł będzie coraz bardziej zyskiwać na znaczeniu przy decyzjach sektora ICT o inwestycjach w regionie. Kwestia wpływu branży na środowisko znalazła w krajach Trójmorza oddźwięk, a rządy i przedsiębiorstwa podjęły pewne wysiłki na rzecz poprawy sytuacji. Ograniczenia rozwoju sektora ICT należy unikać, przyniosłoby ono negatywne skutki, natomiast zmiana źródeł energii zasilającej tę branżę to krok we właściwym kierunku.



Rynek cyberbezpieczeństwa w krajach Trójmorza



Cele Inicjatywy Trójmorza



POTENCJAŁ INNOWACJI W REGIONIE TRÓJMORZA: CYBERBEZPIECZEŃSTWO

Cyberbezpieczeństwo to nie tylko wyzwanie. To także szansa dla tych firm i rynków, które dzięki wiedzy i odwadze innowatorów są w stanie zmieniać reguły gry poprzez nowe spojrzenie na przełomowe technologie. Roczna wartość rynku cyberbezpieczeństwa na świecie szacowana jest obecnie (2019 r.) na 115 do nawet 180 miliardów dolarów. Dominują na nim dostawcy produktów i usług z USA, Izraela czy Wielkiej Brytanii. Jednocześnie marki takie jak Avast (Republika Czeska), ESET (Słowacja) czy Bitdefender (Rumunia) pokazują, że mocne zaplecze techniczne, wykuwane na politechnikach i uniwersytetach Europy Środkowo-Wschodniej, połączone z globalnymi ambicjami przedsiębiorców z regionu, może stanowić podstawę dla przewagi konkurencyjnej produktów z krajów Trójmorza. Jednak zmiany na rynku cyberbezpieczeństwa, jakie zaszły w ostatnich latach, to także wyzwanie dla modeli, które obrały przywołane firmy z regionu – w 2019 r. nie sposób po prostu skopiować ich drogi. O ile koniec XX i pierwsza dekada XXI wieku na rynku IT to czas tradycyjnych firm antywirusowych, takich jak Avast, ESET czy Bitdefender, z ich dużą skalowalnością opartą na w miarę jednorodnym środowisku wielu podobnych stacji roboczych, o tyle aktualnie sektor cyberbezpieczeństwa to znacznie bardziej pofragmentowany rynek, dostarczający wiele różnorodnych kategorii rozwiązań na wielu poziomach i dla wielu grup odbiorców. Od standardowych systemów do zarządzania informacją i zdarzeniami bezpieczeństwa (SIEM), przez usługi w zakresie zarządzania tożsamością użytkowników, rozwiązania dla bezpieczeństwa urządzeń końcowych, Internetu Rzeczy (IoT), chmury obliczeniowej, domen www czy też segment platform *threat intelligence*. Analizując startupy oraz scaleupy z krajów Trójmorza, wskazać można na co najmniej trzy segmenty obiecującej specjalizacji regionalnej:

- bezpieczeństwo systemów przemysłowych opartych o rozproszone urządzenia końcowe – IoT oraz SCADA;
- bezpieczeństwo kodu programistycznego;
- weryfikacja tożsamości.

W wypadku każdej ze wskazanych nisz region Trójmorza posiada określone zasoby, na których zbudować może unikatową na skalę globu wiedzę specjalistyczną. Dla sieci przemysłowych opartych o IoT/SCADA jest to rozbudowany system edukacji inżynierskiej skoncentrowany na wsparciu technicznym instalacji przemysłowych, stanowiący częściowo schedę po systemie ekonomiczno-politycznym sprzed 1989 roku. Dla bezpieczeństwa kodu jest to duża ilość programistów posiadających doświadczenie w pracy w firmach typu *software house* z regionu, świadczących usługi dla klientów z całego świata od prawie dwóch dekad. Z kolei dla weryfikacji tożsamości kluczowym elementem jest dostępny w regionie i otwarty na innowacje sektor fintech, będący pierwszą grupą odbiorców tego typu rozwiązań (tzw. *early adopters*).

W celu szerszego zaprezentowania potencjału innowacji dla cyberbezpieczeństwa przedstawiono w tej części raportu dziesięć wybranych startupów i scaleupów z krajów Trójmorza. Opisane studia przypadków pochodzą z różnych segmentów rynku: od platform zapewniających bezpieczne dzielenie haseł w ramach zespołów przez systemy detekcji zagrożeń po produkty chroniące strony www. Łączy je natomiast jedna cecha wspólna – stoją za nimi zespoły innowatorów z Europy Środkowo-Wschodniej, którzy planują podbić globalny rynek cyberbezpieczeństwa.

BEZPIECZNY ADMIN123

81% incydentów związanych z włamaniami hackerskimi wykorzystuje wykradzione lub słabe hasła jako jeden z wektorów ataku[2]. Zarządzanie własnymi hasłami to już niemałe wyzwanie, a co jeśli w grę wchodzi potrzeba przesyłania haseł współpracownikom z innej strefy czasowej? Bezpieczne przekazywanie tak wrażliwych danych w zespołach pracujących zdalnie stanowi aktualnie jedno z największych wyzwań w branżach takich jak obsługa infrastruktury IT (w tym Business Process Outsourcing), marketing czy tworzenie oprogramowania. Odpowiedzią na ten problem ma być Pass Camp – pierwszy manager haseł zbudowany jednocześnie z myślą o bezkompromisowym bezpieczeństwie i pracy w zespole.

Historia powstania Pass Camp to sztandarowy przykład powiedzenia „potrzeba matką wynalazku". Działająca od 2009 roku na Litwie agencja e-commerce Adeoweb, rozwijając coraz większe projekty, natrafiła na problem związany z brakiem na rynku odpowiedniego narzędzia, które umożliwiłoby im bezpieczne i wydajne dzielenie haseł w ramach zespołów projektowych. Część z rozwiązań rynkowych szła na kompromisy w zakresie bezpieczeństwa, część nie była przystosowana do wykorzystania przez zwykłego użytkownika (słaby UX), innym brakowało z kolei odpowiednich użyteczności. W związku z tym w roku 2015 zespół kilku programistów i ekspertów UX z Adeoweb rozpoczął pracę nad narzędziem, które nie tylko odpowiadałoby potrzebom firmy, ale stało się także działającą rynkowo spółką typu spin-off. Logika tworzenia opierała się na ścisłej współpracy z odbiorcami oraz kolejnych iteracjach przeprowadzanych dzięki informacjom zwrotnym od użytkowników. Na efekty nie trzeba było długo czekać, jeszcze w roku 2017 Pass Camp otrzymał nagrodę Litewskiego Centrum Innowacji za najbardziej innowacyjny produkt w kraju. Oficjalna premiera miała miejsce rok później, a do dnia dzisiejszego już ponad 2000 zespołów wykorzystuje Pass Camp w celu dzielenia haseł.

Produkt opiera się na kluczowej zasadzie – *security first* – realizowanej przez równoczesne wykorzystanie szeregu rozwiązań technologicznych:

- Metodę zero-knowledge proof, która pozwala na potwierdzenie przez użytkownika (klienta), że posiada określony klucz kryptograficzny, bez wysyłania go w całości do odbiorcy (serwera).
- Technologię blockchain zapisującą wszelkie zmiany haseł w zespole.
- Zaawansowane algorytmy kryptograficzne (RSA oraz EAS).

2 Thu Pham, *Stop the Pwnage: 81% of Hacking Incidents Used Stolen or Weak Passwords*, Decipher, 2 maja 2017, [online]: https://duo.com/decipher/stop-the-pwnage-81-of-hacking-incidents-used-stolen-or-weak-passwords.

W praktyce, wszystkie dane przechowywane na serwerach Pass Camp są w całości szyfrowane, a więc niezrozumiałe dla postronnego użytkownika nawet w wypadku wycieku danych czy włamania. Jedyny moment i miejsce, kiedy zostają odszyfrowane, to urządzenie końcowe (klient) po wpisaniu odpowiedniego hasła głównego charakterystycznego jedynie dla określonego użytkownika. Dodatkowo wykorzystanie blockchain zapewnia, że hasło nigdy nie zostanie zgubione lub też złośliwie zmienione, co skutkowałoby możliwością trwałego braku dostępu do pliku. Aktualnie rozwiązanie dostępne jest w formie aplikacji online, zespół zamierza pod koniec 2019 roku opublikować aplikację mobilną, a w 2020 aplikację na komputery biurowe.

Historia projektu Pass Camp pokazuje, że konkretny problem cyberbezpieczeństwa może być nie tylko jednostkowym wyzwaniem, ale też szansą dla innowatorów, którzy umieją dostrzec w nim potencjał rynkowy. Ponad 250 000 haseł i sekretów słanych już poprzez platformę potwierdza ten fakt.

DNA PISANE KLAWIATURĄ

typingdna

Tylko w roku 2017 w samych USA ponad 16 milionów konsumentów stało się ofiarą przejęcia konta. Ich straty pieniężne związane z tym procederem sięgnęły wówczas ponad 5 miliardów dolarów[3]. Zabezpieczenie naszej cyfrowej tożsamości to jedno z kluczowych wyzwań nie tylko w sektorze e-commerce, ale w praktyce w każdej branży korzystającej z usług online od bankowości czy telemedycyny po rynek gier komputerowych. Pomóc może w tym biometria behawioralna, badająca unikalny sposób, w jaki każde z nas korzysta z klawiatury, myszki czy smartfona. TypingDNA to rumuński startup, który w oparciu o to, jak piszemy, jest w stanie stworzyć nasze cyfrowe DNA, które pomoże zabezpieczyć konto czy usługę.

Ile czasu zajmuje nam przejście od określonej litery na klawiaturze do innego znaku, jak długo zatrzymujemy się na określonym klawiszu, w jaki sposób poruszamy myszką czy w końcu jak trzymamy urządzenie mobilne (dane z akcelerometru i żyroskopu) – wszystko to składa się na wzór korzystania z urządzeń cyfrowych przez określonego użytkownika. Informacje te w kolejnym kroku trafiają pod lupę zautomatyzowanych algorytmów, które w procesie analizy danych i uczenia maszynowego tworzą profil poszczególnej osoby. Stanowi on wzór – cyfrowe DNA – z którym porównywana jest przyszła aktywność użytkowników.

TypingDNA oferuje dwa modele weryfikacji tożsamości. Pierwszy z nich opiera się na wpisywaniu tego samego tekstu, np. nazwy użytkownika oraz hasła. W tym wypadku system działa już od 7 znaków, a przy dwóch próbach i 30 znakach może zapewnić 95,4% skuteczności. Drugim modelem jest opcja dowolnego, zmieniającego się tekstu, w której niezbędne jest 100 znaków, a poziom 99% pewności możliwy jest przy 140 uderzeniach w klawiaturę i dwóch podejściach. Co ciekawe przy tak zbudowanej weryfikacji, więcej nie oznacza lepiej – optymalną proporcją jest właśnie 140 znaków, powyżej których precyzja algorytmów znów spada. Tak zbudowana biometria behawioralna stanowi szanse na zwiększenie bezpieczeństwa tożsamości przy równoczesnym braku ingerencji w łatwość użytkowania usługi. Z perspektywy weryfikowanego nie wymaga ona żadnych dodatkowych kroków. W związku z tym stanowi szczególnie praktyczne rozwiązanie w ramach wprowadzania drugiego składnika uwierzytelnienia (2FA), autentykacji opartej o analizę ryzyka czy ciągłego uwierzytelniania.

3 Al Pascual, Kyle Marchini, Sarah Miller, *2018 identity fraud: Fraud enters a new era of complexity*, 6 lutego 2018, [online]: https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity.

Sam startup założony został w 2016 roku i oprócz siedziby głównej w rumuńskiej Oradei posiada także biuro w USA, gdzie w roku 2018 wziął udział w programie akceleracyjnym Techstars. Ważnym krokiem na ścieżce rozwoju firmy był początek 2019 roku, kiedy to TypingDNA zebrał ponad 1,5 miliona dolarów inwestycji w ramach rundy *seed*. Faza wzrostu pozwolić ma startupowi na pozyskanie nowych klientów, szczególnie na rynkach Ameryki Północnej, Europy, ale też Ameryki Południowej. Dynamika rynków globalnych wydaje się potwierdzać optymistyczne prognozy dla segmentu biometrii behawioralnej. Zarówno ze względu na nowe regulacje, jak i wzrastającą świadomość klientów organizacje podnoszą wymagania bezpieczeństwa dotyczące usług online, co stanowi z jednej strony wyzwanie technologiczne dla dostawców usług, ale z drugiej szansę biznesową dla firm takich jak TypingDNA.

BROKER BEZPIECZEŃSTWA DOSTĘPU

SECFENSE

Szacuje się, że na czarnym rynku dostępnych jest ponad 1,9 miliarda skradzionych haseł oraz loginów[4]. Jednocześnie dzięki wykorzystaniu najnowszych technologii, np. uczenia maszynowego, coraz bardziej masowe i skuteczne stają się kampanie ataków phishingowych oraz man-in-the-middle, które pozwalają wyłudzać nasze dane dostępowe. Wszystko to sprawia, że oparcie dostępu do swojej skrzynki e-mail czy konta na portalu społecznościowym jedynie na pojedynczym, nawet odpowiednio skomplikowanym haśle staje się niewystarczające. Niezbędny jest tzw. drugi składnik uwierzytelnienia (2FA). Pytanie, jak wprowadzić go w sposób bezpieczny, szybki i nieingerujący w działanie usługi? Odpowiedzią ma być platforma 2FA tworzona przez firmę Secfense z Polski.

Secfense w praktyce tworzy dodatkową warstwę bezpieczeństwa pośredniczącą w komunikacji i autoryzacji pomiędzy użytkownikiem a samą aplikacją. W ramach tej warstwy umożliwia umieszczenie dowolnej drugiej metody uwierzytelnienia – od biometrii twarzy i kluczy kryptograficznych poprzez aplikacje uwierzytelniające po biometrię behawioralną. Taki model funkcjonowania rozwiązania pozwala dużym organizacjom na wyrwanie się z pułapki uzależnienia od określonego dostawcy 2FA, jednocześnie łącząc istniejącą już w jej ramach infrastrukturę poprzez dodatkową „płachtę bezpieczeństwa". W uproszczeniu tożsamość użytkownika zabezpieczana jest w drodze pomiędzy urządzeniem, z którego korzysta, a usługą, do której chce uzyskać dostęp.

4 Kif Leswing, *There are 1.9 billion stolen passwords and usernames available on the black market*, Yahoo, 13.11.2017, [online]: https://finance.yahoo.com/news/1-9-billion-stolen-passwords-173207888.html?guccounter=1.

Dzięki przyjętemu modelowi Secfense stanowi broker bezpieczeństwa dla firm poszukujących skalowalnego 2FA. Opisywane rozwiązanie pozwala także na wprowadzanie mikro-autoryzacji określonych dostępów lub działań jako metody zabezpieczającej szczególnie wrażliwe zasoby. Jest to możliwe bez potrzeby ingerencji w kod aplikacji bądź strukturę usługi – wszelkie reguły stosowane są „w locie", pomiędzy użytkownikiem a zasobami.

W ramach przeprowadzanych aktualnie wdrożeń *proof of concept* (POC) rozwiązanie testuje m.in. operator największego systemu transportowego w Polsce. Jednocześnie, będąc platformą integrującą różne rozwiązania technologiczne dla drugiego składnika uwierzytelnienia, Secfense to także rynek i kanał dotarcia dla producentów poszczególnych 2FA. Wśród partnerów startupu z tego segmentu rynku znajdziemy m.in. twórców myszy biometrycznych Cherry oraz firmę dostarczającą usługi w zakresie biometrii twarzy, Iproof. Sam Secfense założony został w 2018 roku w Krakowie. Aktualnie, po inwestycji na poziomie 850 000 dolarów pochodzącej z lokalnego ekosystemu, zespół rozpoczyna przygotowania do ekspansji międzynarodowej.

PLIKI POD NADZOREM

Olympus Sky

Brak odpowiedniej ochrony plików gromadzonych oraz przetwarzanych w organizacji stanowi często piętę achillesową całego systemu bezpieczeństwa. Potwierdzają to przykłady wycieków z takich firm jak Adidas czy LinkedIn. Małe i średnie przedsiębiorstwa także stają się coraz częściej ofiarami tego typu naruszeń bezpieczeństwa, jak pokazują badania nawet w 43% ze wszystkich przypadków[5]. Odpowiedzią na to wyzwanie ma być *File Guard*, rozwiązanie tworzone przez firmę Olympus Sky z Polski.

Bezpieczeństwo plików stanowi jeden z trudniejszych elementów zarządzania danymi przetwarzanymi w organizacji. Potencjalnie dostępne na rynku narzędzia w większości wypadków wymagają od użytkowników szeregu dodatkowych czynności, przez co ograniczają produktywność pracowników, zniechęcając ich także do korzystania z samych rozwiązań. Logika stojąca za *File Guard* jest w tym kontekście prosta – pełne bezpieczeństwo przy jednoczesnej minimalnej ingerencji w procesy biznesowe. Z perspektywy użytkownika jedno kliknięcie myszy pozwala na uruchomienie ochrony, drugie na ustalenie osób, które mają mieć dostęp do pliku. I tyle – zasoby nie muszą być przenoszone do żadnych „bezpiecznych przestrzeni dyskowych", pracownik nie musi generować żadnego dodatkowego hasła, a w wypadku rozwiązań w chmurze integracja odbywa się automatycznie. Bezpieczeństwo ukryte jest w technologii stanowiącej rdzeń File Guard – autonomicznym zarządzaniu kluczami (ang. *Autonomous Key Management*, AKM).

Większość rozwiązań zabezpieczających komunikację oraz przesyłanie danych opiera się obecnie na infrastrukturze klucza publicznego wykorzystującej certyfikaty cyfrowe. Sprawdza się ona

5 Verizon, *2019 Data Breach Investigations Report*, 2019, [online]: https://enterprise.verizon.com/resources/executivebriefs/2019-dbir-executive-brief.pdf.

idealnie w kontekście bankowości internetowej czy wymiany maili, jednak okazuje się niepraktyczna w wypadku ochrony rozproszonych sieci takich jak pliki w organizacjach czy IoT. W odpowiedzi na te wyzwania Olympus Sky rozwija autorską technologię pozwalającą na autonomicznie zarządzanie kluczami. Opiera się ona na zdecentralizowanej sieci, którą tworzą wszystkie podłączone do niej węzły końcowe, w czasie rzeczywistym komunikujące się ze sobą w celu potwierdzenia swoich poświadczeń bezpieczeństwa. Rozwiązanie wykorzystuje podobną logikę jak technologia blockchain, jednak nie jest tak skomplikowane oraz obciążające dla systemu, przez co może funkcjonować w większych sieciach łączących małe podmioty. W wypadku ochrony plików zapewnia ono unikalny klucz kryptograficzny dla każdego pliku oraz jego ciągłe odświeżanie w celu zapewnienia autentyczności. Dodatkowo klucze przechowywane są na urządzeniach firmowych, nawet w wypadku integracji z chmurą.

Technologia AKM oprócz *File Guard* znalazła swoje zastosowanie w drugim produkcie polskiej firmy, platformie Zeus dedykowanej bezpieczeństwu sieci IoT. Zeus był testowany w ramach wdrożeń *proof of concept* m.in. w Bombardierze czy Magno Electronic, a także w ramach projektu B+R w Boeing Aerospace. Sama firma Olympus Sky oprócz siedziby w Łodzi posiada też biuro w San Diego, a dzięki 1,8 miliona dolarów inwestycji planuje rozszerzenie działalności na kolejne sektory. Ostatecznie, jak pokazują predykcje rynku bezpieczeństwa, w kolejnych latach liczba niezabezpieczonych urządzeń IoT czy plików będzie jedynie rosła[6].

avatao

ZAKODOWANE BEZPIECZEŃSTWO

Statystycznie każda aplikacja posiada około 10 podatności wynikających z błędów popełnionych na etapie pisania jej kodu. Koszty poniesione przez twórców oprogramowania związane z wykryciem takiego bugu wahają się w zależności od etapu: od 1500 dolarów podczas testowania po nawet 10 000 w trakcie fazy produkcyjnej. Nie wspominając nawet o potencjalnych stratach po stronie użytkowników, które mogą sięgać milionów dolarów. Odpowiedzią na tak nakreślone wyzwanie ma być węgierska platforma Avatao, która poprzez odpowiednio skrojone treningi pozwala zespołom deweloperów wdrażać wymagania bezpieczeństwa w procesy tworzenia oprogramowania.

Software staje się kluczowym pośrednikiem w naszych codziennych aktywnościach – od jego bezpiecznej architektury uzależniona jest coraz większa ilość ważnych dla nas elementów: danych, pieniędzy czy krytycznych procesów. Jednocześnie kody aplikacji, z których korzystamy, stają się coraz dłuższe i bardziej skomplikowane, a co za tym idzie, statystycznie muszą posiadać więcej błędów bezpieczeństwa. Przeglądarka Google Chrome to ponad 6 milionów linii kodu, system operacyjny Windows 7 – około 40 milionów, a system operacyjny Mac OS X – 85 milionów. Oprogramowanie współczesnego samochodu to średnio 100 milionów

6 IoT Security Foundation, *Report: Insecurity in the Internet of Things*, 2015, [online]: https://www.iotsecurityfoundation.org/tag/report/.

linii kodu[7]. Dla zobrazowania skali warto wskazać, że jeden milion linii kodu to około 18 000 zapisanych stron formatu A4. Nic więc dziwnego, że w trakcie jednego tygodnia swojej pracy deweloperzy spędzają średnio osiem godzin na poprawianiu bugów w tworzonych aplikacjach.

Aby zapewnić bezpieczeństwo kodu, firmy programistyczne korzystać mogą z odpowiednich narzędzi – skanerów, które w oparciu o algorytmy automatycznie starają się wykryć i naprawić pomyłki deweloperów. Mowa o tzw. rozwiązaniach SAST (*Static Automated Software Testing*) oraz DAST (*Dynamic Automated Software Testing*). Jednak jak pokazują historie kolejnych odkrywanych podatności, automatyczna analiza nie jest w stanie wychwycić bardziej skomplikowanych zależności oraz potencjalnych słabych punktów kodu. W tym miejscu wkroczyć musi człowiek.

Tworzenie kodu aplikacji zgodnie z zasadą *secure by design* jest zadaniem nie dla wybranego specjalisty od cyberbezpieczeństwa, ale dla całego zespołu programistów. Wyzwaniem staje się zatem nie tyle jednorazowe dostarczenie odpowiedniej wiedzy deweloperom, ile ciągłe doszkalanie ich oraz aktualizacja realnych umiejętności. W tym celu powstała platforma Avatao, która w oparciu o środowisko zbudowane w chmurze i dostępne dla każdego użytkownika poprzez przeglądarkę dostarcza już ponad 850 sesji ćwiczeniowych. Zakres tematyczny zadań dotyczy wszystkich najważniejszych kwestii związanych z bezpieczeństwem programowania, a także kluczowych języków takich jak Java, Python, C#, C++, PHP i inne. Co ważne, platforma aktualizowana jest co miesiąc około 20 nowymi ćwiczeniami. Przyjmują one jedną z dwóch form: dla mniej zaawansowanych tutorial ze wsparciem chat bota, dla bardziej wymagających wyzwania do wykonania (np. znajdź lukę w ramach kodu) bez jakiejkolwiek podpowiedzi. Zadaniem tak skonstruowanej platformy jest wspieranie logiki kodowania opartego na bezpieczeństwie, ale także umożliwienie monitorowania rozwoju pracowników oraz zarządzania ich nowymi umiejętnościami przez managerów. Sama Avatao powstała w 2014 w Budapeszcie jako projekt znanego w branży cyberbezpieczeństwa Laboratory of Cryptography and System Security (CrySyS Lab) na Budapest University of Technology and Economics. Jej dynamiczny rozwój rozpoczął się po 2016 roku dzięki pierwszym inwestycjom aniołów biznesu i funduszy VC. W roku 2018 firma zdecydowała się na ekspansję na rynek amerykański. Aktualnie platforma posiada ponad 10 000 aktywnych użytkowników, głównie w Europie Zachodniej oraz USA. W ich gronie znaleźli się m.in. LogMeIn czy Lufthansa Systems. Korzystając z Avatao, są oni w stanie obniżyć koszty związane z naprawą bugów w procesie produkcyjnym o nawet 30%. W dobie zmian rynku pracy związanych z automatyzacją Avatao jest także obiecującym przykładem, który potwierdza, że algorytm nie zastąpi wszystkich umiejętności człowieka, nawet w tak cyfrowej branży jak tworzenie oprogramowania.

7 David McCandels, *Codebases*, 2015, [online]: https://informationisbeautiful.net/visualizations/million-lines-of-code/.

iTOŻSAMOŚĆ

iDenfy

Według danych za rok 2018 ponad 14 milionów konsumentów padło ofiarą kradzieży tożsamości w samych tylko Stanach Zjednoczonych[8]. Podszywanie się pod innych lub też tworzenie całkowicie fikcyjnych osobowości staje się także coraz poważniejszym wyzwaniem dla świadczenia wielu usług cyfrowych. Szereg branż takich jak gry online, gospodarka współdzielenia czy fintech opiera swój model biznesowy na zdalnym potwierdzaniu tożsamości użytkownika. Odpowiedzią na ich problemy ma być iDenfy z Litwy.

8 Kyle Marchini, Al Pascual, *2019 Identity Fraud Study: Fraudsters Seek New Targets and Victims Bear the Brunt*, 6 marca 2019, [online]: https://www.javelinstrategy.com/coverage-area/2019-identity-fraud-study-fraudsters-seek-new-targets-and-victims-bear-brunt.

Pierwsze trzy kroki w ramach procesu potwierdzania tożsamości dzieją się po stronie użytkownika. Musi on podać niezbędne dane, takie jak np. imię, nazwisko czy wiek, wypełniając prawne wymogi związane z samodzielnym określeniem danych osobowych. W drugim kroku poprzez aplikacje użytkownik robi sobie selfie. W rzeczywistości jest to seria zdjęć, która pozwala zarówno na potwierdzenie, że mamy do czynienia z realną, żywą osobą a nie botem, jak i wyciągnięcie danych biometrycznych niezbędnych do procesu rozpoznawania twarzy. Jest to element szczególnie newralgiczny w kontekście coraz popularniejszego procesu tworzenia przez algorytmy AI zdjęć osób realnie nieistniejących[9]. W trzecim kroku klient wykonuje zdjęcie dokumentu, np. dowodu tożsamości, a dzięki zastosowaniu optycznego rozpoznawania pisma (*optical character recognition*, OCR) można automatycznie sczytać jego dane. Ostatni, kluczowy element całego procesu odbywa się już po zaszyfrowaniu i przesłaniu danych na serwer iDenfy. Z wykorzystaniem szeregu algorytmów i przy wspomaganiu uczenia maszynowego dostarczony zestaw informacji jest badany pod kątem:

- Czy wpisane dane pokrywają się z danymi z dokumentu?
- Czy osoba ze zdjęcia to ta sama osoba co na dokumencie?
- Czy podana osoba spełnia wymogi specyficzne dla określonej usługi – np. związane z wiekiem, posiadaniem licencji na określone działania lub prawa do prowadzenia pojazdów czy też zgodnością z wytycznymi w sprawie zwalczania prania pieniędzy.

Dodatkowo produkt umożliwia także rozszerzenie weryfikacji tożsamości w razie potrzeby o elementy procesów „znaj swojego klienta" (KYC), *customer due diligence*, czy nawet *enhanced due diligence*. Aktualnie rozwiązanie wspiera rozpoznawanie ponad 900 rodzajów dokumentów wykorzystywanych w 195 krajach, co oznacza w praktyce globalny zasięg usługi.

Sam iDenfy to spin-off, który powstał na Uniwersytecie Technologicznym w Kownie dzięki programowi inkubacyjnemu prowadzonemu tam przez Kowieński Park Naukowo-technologiczny. Z ponad 20 pracownikami i 50 klientami startup szykuje się aktualnie do szerszej ekspansji międzynarodowej oraz rundy inwestycyjnej na poziomie serii A. Z usług iDenfy skorzystały już m.in. Bank Narodowy na Litwie, MOQ (płatności mobilne), TopSpot (platforma dla graczy online) czy EveryMatrix (kasyno oraz bukmacher online). Podsumowując trend, w który wpisuje się litewska firma – czy nam się to podoba czy nie, w cyfrowym świecie zaufanie do klienta w coraz większej mierze oparte jest na technologii oraz dużych zbiorach danych.

9 Przykładem może być strona www thispersondoesnotexist.com.

NA STRAŻY INTERNETU

WEBTOTEM
Security Monitoring

Statystyczna strona internetowa była w roku 2018 celem średnio 62 ataków tylko w ciągu jednego dnia. Automatyzacja działań ofensywnych na domeny www w ostatnich latach stała się powodem znacznego wzrostu ilości ataków, tylko od stycznia do grudnia 2018 o 59%[10]. Masowy charakter zagrożenia wymaga działań zaradczych zakrojonych na szeroką skalę, wykorzystujących m.in. algorytmy uczenia maszynowego, a także inne technologie wspierające administratorów i specjalistów od bezpieczeństwa. Podejmuje je m.in. estoński startup WebTotem, chroniący już 149 544 stron www na całym świecie.

Bezpieczeństwo witryn staje się jednym z kluczowych wyzwań dla sprawnego funkcjonowania coraz większej ilości usług cyfrowych dostarczanych poprzez aplikacje webowe. Jak pokazują badania, aktualnie ponad 45% stron www posiada podatność, którą zakwalifikować można jako poważną, a aż 87% domen lukę bezpieczeństwa powodującą niższy stopień zagrożenia. W około 30% strony podatne są na Cross-site Scripting (XSS), inne luki to m.in. wykorzystanie podatnych bibliotek Javascript oraz nieodpowiednie wdrożenie WordPress pozostawiające możliwość udanego użycia exploita[11]. Oprócz problemu luk w zabezpieczeniach stron domeny narażone są także na ataki oparte na masowych operacjach przekierowywania ruchu internetowego w celu uniemożliwienia dostępu do nich – tzw. Distributed Denial of Service (DDoS). Ataki takie mimo oparcia się jedynie na „brutalnej sile" są w stanie uniemożliwić dostęp do usług publicznych czy nawet bankowych obywatelom i konsumentom, czego przykładem był np. kryzys estoński z roku 2007. W ostatnich latach ataki DDOS przybierają także na sile, m.in. ze względu na wykorzystanie w procesie ich przeprowadzania coraz większej ilości urządzeń IoT podłączonych do sieci.

Opisane zagrożenia stanowią także wyzwanie dla krajów Europy Środkowo-Wschodniej. W ramach przekrojowej analizy domen narodowych krajów bałtyckich – Estonii, Litwy, Łotwy – obejmującej łącznie ponad 200 tysięcy stron www WebTotem wykrył 946 zainfekowanych witryn.

Sam startup WebTotem zapewnia cały łańcuch działań, od biernej ochrony z wykorzystaniem Web Application Firewall, przez ciągły monitoring pod kątem szeregu zagrożeń takich jak podatności, skanowanie portów czy *malware*, po aktywną odpowiedź, gdy wykryte zostaje zagrożenie. Firma posiada ponaddwudziestoosobowy zespół obsługi incydentów komputerowych (Computer Emergency Response Team, CERT) pracujący z Kazachstanu. Obecnie usługa oferowana jest bezpłatnie właścicielom do 10 stron internetowych. Cel tak skonstruowanego modelu biznesowego to ochrona jak największej ilości stron www na całym świecie. Umożliwia to pozyskiwanie i analizę informacji o zagrożeniach, a co za tym idzie, lepsze uczenie algorytmów sztucznej inteligencji stojących za produktem. W kolejnym kroku odpowiednio przygotowane algorytmy oferowane są odpłatnie dla ochrony klientów poziomu *enterprise*, szczególnie z sektora finansowego oraz IT.

10 Curtis Jr. Franklin, *Website Attack Attempts Rose by 69% in 2018*, DARKReading, 2019, [online]: https://www.darkreading.com/vulnerabilities---threats/website-attack-attempts-rose-by-69--in-2018/d/d-id/1334714.

11 Acunetix, *Web Application Vulnerability Report 2019*, 2019, [online]: https://cdn2.hubspot.net/hubfs/4595665/Acunetix_web_application_vulnerability_report_2019.pdf.

PRAWO DO BYCIA USUNIĘTYM

Niewielu użytkowników systemów operacyjnych takich jak Windows zdaje sobie sprawę, że wybranie opcji „usuń" lub naciśnięcie przycisku *delete* w praktyce nie niszczy pliku, którego chcemy się pozbyć. Zabieg ten uniemożliwia dostęp do niego, jednak przy zastosowaniu odpowiednich narzędzi istnieje możliwość odzyskania danych wciąż zapisanych na dysku twardym komputera. W wypadku wrażliwych informacji stanowi to realne zagrożenie, także w kontekście coraz szerszych regulacji dotyczących bezpiecznego przetwarzania danych osobowych. Rozwiązanie Eraser stworzone przez rumuńską firmę East-tec stanowić ma wsparcie w tym zakresie, umożliwiając użytkownikowi przejęcie kontroli nad procesem usuwania danych cyfrowych.

Całkowite usuwanie danych zapisanych na nośnikach cyfrowych oznacza w praktyce nadpisywanie w określony sposób nowych danych na sektorach pamięci zajmowanych przez informacje, które chcemy permanentnie zniszczyć. Szereg instytucji publicznych, ale też ekspertów cyberbezpieczeństwa stworzyło własne standardy algorytmów usuwających dane. Do najbardziej znanych zaliczyć można wykorzystywany przez Departament Obrony USA „DoD 5220.22-M, ECE", który wykonuje proces nadpisywania siedem razy, stworzony przez Federalny Urząd Bezpieczeństwa Informacji w Niemczech „BSI-2011-VS" nadpisujący dane czterokrotnie czy też algorytm Bruce'a Schneiera oparty na siedmiu iteracjach.

Program East-tec Eraser wykorzystuje 14 rodzajów algorytmów usuwających dane. Wszystkie dostępne są dla użytkownika w zależności od jego potrzeb – te działające dłużej oraz obciążające bardziej system operacyjny zapewnić mogą nawet 100% pewności w zakresie wykasowania danych. Oprócz manualnego użycia przez wskazywanie określonych plików, program umożliwia automatyczne usuwanie danych tworzonych przez określone programy i aplikacje. Są to dane pozostawiane w pamięci komputera, o których często nie mamy nawet wiedzy jako użytkownicy. Przykładem może być ilość informacji, jakie wytwarza przeglądarka internetowa, a których użytkownik, nawet ten dbający o swoją prywatność, nie jest w stanie kontrolować. Pomocą ma być w tym wypadku produkt firmy z Rumunii, który aktualnie wspiera usuwanie śladów funkcjonowania ponad 300 aplikacji.

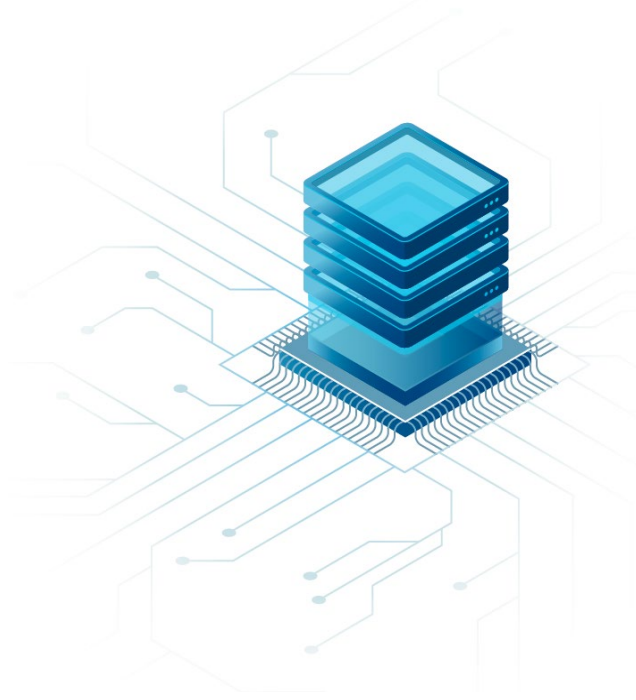
Sam East-tec to MŚP funkcjonujący na rynku już od 1997 roku, kiedy to dwóch założycieli, wówczas jeszcze w szkole średniej, zdecydowało o prowadzeniu z rumuńskiej Oradei globalnej spółki skupionej na bezpieczeństwie i prywatności online. Aktualnie firma posiada szereg produktów, z których ponad 40% sprzedaje w Stanach Zjednoczonych, około 30% w Europie Zachodniej i w coraz większym zakresie w Europie Środkowo-Wschodniej. W kontekście nowych regulacji dotyczących danych, takich jak np. RODO, znaczenie zarządzania całym cyklem życia informacji cyfrowej staje się ważnym elementem polityk bezpieczeństwa i prywatności. W związku z tym „prawo do bycia usuniętym", które oferuje East-tec, przestaje być domeną pasjonatów czy ekspertów, a staje się podstawowym prawem konsumenta i obywatela.

PUNKT POCZĄTKOWY BEZPIECZNEJ SIECI

Ponad 70% naruszeń bezpieczeństwa w świecie cyfrowym bierze swój początek z niedostatecznie chronionych punktów końcowych sieci – komputerów, smartfonów czy drukarek[12]. Jednocześnie, jak pokazują badania, firmy w wielu wypadkach przepłacają za ochronę tego segmentu sieci, nie uzyskując odpowiednich efektów. Często wpadają wręcz w pułapkę, w której większy budżet przekłada się na zmniejszoną efektywność zabezpieczenia urządzeń końcowych[13]. Ucieczką z niej ma być „inteligentna" ochrona, jaką oferuje platforma Trapmine Defense z Estonii, oparta na uczeniu maszynowym oraz analizie behawioralnej.

Zabezpieczenie sieci firmowej w roku 2019 to całkiem inne wyzwanie dla administratora niż jeszcze niecałe 5 czy 8 lat temu. W dobie masowego wykorzystywania formuły „przynieś swoje własne urządzenie" (*bring your own device*, BYOD), a także coraz szerszych zastosowań Internetu Rzeczy (IoT), czy jak niektórzy wręcz wskazują „Internetu wszystkiego" (*Internet of everything*), rozgraniczenie na sieć wewnętrzną i zewnętrzną staje się trudne do utrzymania. Budowanie murów dookoła cyfrowych zasobów firmy w postaci firewalli i innych statycznych przeszkód przestaje być wydajne – atakujący nie muszą szukać w nich dziur, po prostu je obchodzą. W związku z tym coraz większy segment rynku cyberbezpieczeństwa skupia się na dynamicznej analizie środowiska w celu wyłapywania i zablokowania podejrzanych zjawisk.

Estońska platforma Trapmine Defense umożliwia ochronę urządzeń końcowych przed zagrożeniami ze strony klasycznych plików malware, ataków bezplikowych, a nawet celowanych kampanii takich jak np. ransomware. Swoje działanie opiera nie na zbiorze sygnatur określających zamknięty zestaw podejrzanych plików, ale na aktywnej analizie środowiska w poszukiwaniu nienaturalnych zachowań sieci w celu zapewnienia detekcji, prewencji oraz odpowiedzi na potencjalne zagrożenie. Kluczowym elementem jest także wizualizacja sieciowa oraz czasowa ataków, pokazująca administratorowi wektory działań ofensywnych, ich dynamikę oraz specyfikę. W skrócie zadaniem platformy jest nie tylko zautomatyzowanie działań obronnych przy pomocy algorytmów sztucznej inteligencji, ale także stworzenie z dużej masy danych cyfrowych klarownego i aktualnego obrazu sieci, na podstawie której ekspert IT może podjąć odpowiednie działania.



12 Louis Columbus, *5 Key Insights From Absolute's 2019 Endpoint Security Trends Report*, "Forbes", [online]: https://www.forbes.com/sites/louiscolumbus/2019/09/08/5-key-insights-from-absolutes-2019-endpoint-security-trends-report/.

13 Absolute, *2019 Endpoint Security Trends Report*, 2019, [online]: https://www.absolute.com/go/study/2019-endpoint-security-trends/.

Sam Trapmine to startup, który rozpoczął działalność w roku 2016 i dzięki inwestycji aniołów biznesu z Estonii oraz Danii rozwija sprzedaż poprzez siedzibę główną w Tallinie oraz ulepsza algorytmy w centrum R&D w Stambule. Produkt zdobył już klientów na takich rynkach jak Wielka Brytania, Estonia, Indie czy Azerbejdżan. Wdrożenia Trapmine, a także szerzej, produktów z całego segmentu rozwiązań opartych na uczeniu maszynowym potwierdzają, że w kolejnych latach za nasze cyberbezpieczeństwo odpowiadać będą nie pojedynczy, nawet najlepsi specjaliści IT, ale zespoły zbudowane z ludzi i algorytmów.

MAŁE I ŚREDNIE CYBERBEZPIECZEŃSTWO

NISPS

Przedsiębiorcy, bardziej niż jakakolwiek inna grupa zawodowa, powinni być świadomi tego, że wkraczamy w erę cyfrowej rewolucji, w której informacje stały się nową walutą. Jesteśmy coraz bardziej zależni od bezpieczeństwa naszych danych. Mimo to, według badania *Cyber Threat Report CEE 2018* przeprowadzonego wśród przedstawicieli MŚP z Europy Środkowo-Wschodniej, aż 65% firm z regionu nie ma opracowanej strategii cyberbezpieczeństwa, tylko połowa z nich tworzy regularnie kopie danych, a niemal 60% wciąż stawia przede wszystkim na klasyczne oprogramowanie antywirusowe. Wsparciem dla sektora MŚP w zakresie ich bezpieczeństwa w cyberprzestrzeni ma być platforma NISPS stworzona przez firmę ESTEQ z Litwy.

Opisane powyżej braki w przygotowaniu MŚP do walki z atakami cyfrowymi sprawiają, że średni czas detekcji zagrożenia, które znalazło się już w sieci firmy, wynosi trzy miesiące. Sytuacja ta wynika w znacznej mierze z braku odpowiednich budżetów na cyberbezpieczeństwo. Zbudowanie wewnętrznych zdolności lub rozwiązań po prostu kosztuje i okazuje się poza zasięgiem 10- czy 20-osobowego przedsiębiorstwa. Dlatego też cyberbezpieczeństwo MŚP powinno być postrzegane nie jako wyzwanie techniczne, ale jako element procesu biznesowego, i tak też zarządzane. Analiza ryzyka w firmie – jakie dane przetwarzamy cyfrowo, jakie zasoby należy chronić – powinna stanowić pierwszy krok do kolejnych działań: analizy budżetu oraz analizy rynku dostępnych produktów i usług. Dopiero zderzenie wymagań bezpieczeństwa, z dostępnym budżetem i ofertą rynku, mogą pozwolić przedsiębiorstwu na wybranie optymalnej formy zabezpieczenia się – od zakupu elementów hardware na biurka pracowników przez oprogramowanie bądź usługi SaaS po outsourcing określonych elementów. Jednym z takich rozwiązań dedykowanych dla MŚP jest właśnie platforma NISPS.

NISPS, czyli Network Intelligence, Security and Protection Service, opiera się na zasadzie *reversed-proxy*, stanowiąc niejako bufor między cyberprzestrzenią a infrastrukturą przedsiębiorstwa. Wykorzystując taką architekturę, platforma oferuje szereg usług w zależności od potrzeb klienta – firewall, zaawansowaną ochronę DDoS, zautomatyzowaną analizę trendów czy analizę logów. NISPS umożliwia także integrację rozwiązań innych producentów w ramach dostarczanej przez nich usługi, czego przykładem jest współpraca ze słowacką firmą ESET. Samo przedsiębiorstwo ESTEQ, które stworzyło NISPS, powstało w 2014 roku na Ukrainie, a dwa lata później przeniosło siedzibę główną do Wilna na Litwie. Aktualnie sprzedaż koncentruje się na rynku Europy Środkowo-Wschodniej oraz krajach nordyckich. Biorąc pod uwagę, że w samej Unii Europejskiej funkcjonuje ponad 22 miliony MŚP[14], wyzwaniem w ramach rozwiązań dla tego segmentu rynku staje się skalowalność oraz możliwość automatyzacji dostarczania usług przy równoczesnym zachowaniu cen dostosowanych do budżetów. Próbą połączenia tych elementów jest właśnie NISPS.

14 Komisja Europejska, *Small and medium-sized enterprises: an overview*, 2018, [online]: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/EDN-20181119-1.

GEOPOLITYCZNY KRAJOBRAZ CYBERZAGROŻEŃ W REGIONIE EUROPY ŚRODKOWO-WSCHODNIEJ

Krajobraz cyberbezpieczeństwa regionu Europy Środkowo-Wschodniej (dalej: EŚW, region) kształtują przede wszystkim dwa typy czynników. Po pierwsze uwarunkowania geopolityczne, które silnie determinują charakter wyzwań. Po drugie ogólne, globalne trendy związane z zagrożeniami, które nie omijają tej części Europy.

Kluczem do zrozumienia bezpieczeństwa regionu jest dostrzeżenie istnienia bardzo silnej korelacji między sytuacją geopolityczną a cyberzagrożeniami. Najpoważniejsze w skutkach ofensywne działania prowadzone w cyberprzestrzeni nie są nigdy celem samym w sobie, są narzędziem do realizowania celów szerszych, bardzo często strategicznych. Dlatego właśnie, myśląc o cyberbezpieczeństwie poszczególnych krajów, należy zawsze myśleć w wielowymiarowych ramach uwarunkowań bezpieczeństwa narodowego.

BEZPIECZEŃSTWO, OBRONA I STABILNOŚĆ POLITYCZNA

Region EŚW położony jest w niezwykle wrażliwym politycznie obszarze, stanowiąc zewnętrzną granicę zarówno UE, jak i NATO. Sytuację definiuje przede wszystkim sąsiedztwo z Rosją, państwem przejawiającym rewizjonistyczne apetyty i traktującym region jako szczególną strefę swoich wpływów. Jak pokazuje wiele przykładów z niedalekiej przeszłości i wskazuje wiele źródeł, Rosja oraz podmioty przez Kreml wspierane bardzo aktywnie używają narzędzi cyfrowych do realizacji swoich interesów politycznych, militarnych i ekonomicznych, szczególnie wobec krajów sąsiedzkich[15].

Fakt ten przejawia się w różnego typu działaniach, jednym z nich jest szpiegostwo prowadzone w cyberprzestrzeni, nakierowane na kluczowe podmioty publiczne i decyzyjne. Ilustracją problemu może być ujawniona przez firmę FireEye kampania szpiegowska prowadzona przez grupę APT28, wedle firmy bezpośrednio łączona z rosyjskim wywiadem wojskowym. APT28 pozyskiwała informacje na temat rządów, podmiotów politycznych, sektora obronności oraz organizacji zajmujących się bezpieczeństwem takich jak NATO czy OBWE[16]. W obszarze szczególnego zainteresowania znalazły się podmioty z państw EŚW. Korzyści z pozyskanych informacji są szerokie: mogą budować strategiczną świadomość sytuacyjną, a dzięki temu przewagę nad rywalami, mogą także zostać wykorzystane do dalszych wrogich operacji (np. dezinformacyjnych).

Jednak cyberprzestrzeń daje możliwość realizowania działań o skutkach dalece poważniejszych niż te związane z cyberszpiegostwem. Ostatnie lata przyniosły bardzo silny wzrost napięć w regionie EŚW z kulminacyjnym momentem wybuchu konfliktu na Ukrainie w 2014 r. Wielowymiarowe działania ofensywne prowadzone w cyberprzestrzeni stały się regularnie wykorzystywanym orężem w ramach prowadzonych operacji hybrydowych, uświadamiając krajom regionu, jak ważnym zadaniem jest zapewnianie cyberbezpieczeństwa. Szczególnie cyberatak na system energetyczny Ukrainy, który sparaliżował w grudniu 2015 roku jego funkcjonowanie, głównie w regionie Iwano-Frankiwska, stał się kolejnym dowodem, jak bardzo bezpieczeństwo narodowe, przede wszystkim infrastruktura krytyczna, uzależnione jest od wysokiego poziomu cyberbezpieczeństwa.

Jedną z konsekwencji kryzysu bezpieczeństwa na wschodzie była decyzja o wzmocnieniu wschodniej flanki NATO. Wojska stacjonujące w krajach regionu stały się przedmiotem wielowymiarowych wrogich

15 Powszechnie znane cyberataki na Estonię z 2007 i Gruzję z 2008 roku są dziś flagowymi przykładami tego, jak konflikty związane ze światem fizycznym przenoszą się do sieci.

16 FireEye, APT28: *A Window into Russia's Cyber Espionage Operations?*, 2014, [online]: https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

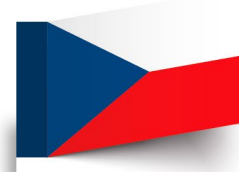
działań prowadzonych przy użyciu narzędzi teleinformatycznych. Hakowanie smartfonów żołnierzy[17] stanowiło przykład ataków o charakterze szpiegowskim. Innymi działaniami były wrogie operacje informacyjne wykorzystujące cyberprzestrzeń. Ich cele były szerokie, między innymi: od wywoływania konfliktów między państwami sojuszniczymi, przez podważanie wiary i zaufania w siłę i determinację Sojuszu w zakresie budowania bezpieczeństwa, aż do obniżenia poziomu akceptacji społecznej dla obecności wojsk NATO na terenie ich państw. Przykładem takiej operacji było rozprzestrzenianie fałszywych informacji na temat gwałtu dokonanego na kobiecie przez żołnierzy stacjonujących na Litwie[18]. Należy się spodziewać, że wraz z planowanym wzrostem ilościowym i jakościowym wojsk rozlokowanych przy granicach zewnętrznych Sojuszu wielowymiarowe cyberoperacje ofensywne będą się nasilać.

Warto zauważyć, że operacje informacyjne, w tym dezinformacyjne, prowadzone w cyberprzestrzeni są wykorzystywane w bardzo szerokim zakresie, wykraczającym poza kwestie stricte militarne. Często stanowią narzędzie służące między innymi do tworzenia napięć politycznych, polaryzacji społecznej, obniżania zaufania do władzy itd. Istotną cechą charakterystyczną jest to, że zazwyczaj dostosowywane są do lokalnych uwarunkowań i poruszają wątki czy kwestie wrażliwe społecznie w poszczególnych krajach. Przeprowadzenie „szytych na miarę" działań umożliwia właśnie wykorzystanie narzędzi cyfrowych. Poniższy graf pokazuje wybrane wątki dominujące w narracjach wykorzystywanych w kampaniach dezinformacyjnych, prowadzonych także w sieci w państwach regionu lub przeciwko nim.

TEMATY I NARRACJE WE WROGICH KAMPANIACH DEZINFORMACYJNYCH WYMIERZONYCH W PAŃSTWA REGIONU

POLSKA

- narracje antyukraińskie
- obniżenie wiary w NATO
- atomizacja społeczeństwa
- narracja antyzachodnia



CZECHY

- islamizacja Europy
- USA to agresywne państwo
- Ukraina to państwo upadające
- bezradny, skorumpowany Zachód
- wzbudzanie nastrojów ksenofobicznych
- kryzys migracyjny

MOŁDAWIA

- upadająca UE
- Zachód jest agresywny
- Rosja jest obrońcą tradycyjnych wartości
- politycy są sterowani przez siły zewnętrzne

17 Mark Moore, *Russia has been hacking smartphones of NATO troops*, 2017, [online]: https://nypost.com/2017/10/04/russia-has-been-hacking-smartphones-of-nato-troops/.

18 Fake.org, *Russia uses fake rape stories to create hostility to NATO troops*, 2018, [online]: https://www.stopfake.org/en/russia-uses-fake-rape-stories-to-create-hostility-to-nato-troops/.

WĘGRY

- kryzys migracyjny
- narracja anty-UE, anty-NATO, anty-USA
- Ukraina to upadające, faszystowskie państwo

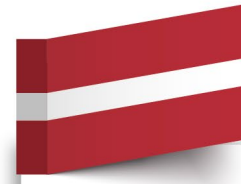
SŁOWACJA

- chaotyczna, bezradna UE
- narracja anty-NATO
- pozytywna rola Rosji na Ukrainie
- skorumpowany Zachód

LITWA

- kraj niewart obrony sojuszniczej
- bliskość światopoglądowa z Rosją
- sentymenty antypolskie
- sentymenty pronazistowskie

ŁOTWA



- sentymenty pronazistowskie
- wsparcie dla Rosji, która buduje stabilizację
- kraj, którego miejsce jest poza UE

UKRAINA

- okrucieństwa wojenne
- państwo upadłe
- krajem rządzi chaos
- zmiany polityczne były sterowane przez Zachód
- poparcie międzynarodowe po stronie rosyjskiej
- kraj rządzony przez faszystów

ESTONIA

- wzmacnianie działań wymierzonych w mniejszości
- sentymenty pronazistowskie

Źródło: Opracowanie własne na podstawie: Centre for International Relations & Partners, *Information warfare in the Internet: Countering pro-Kremlin disinformation in the CEE countries*, 2017 oraz CEPA, *Winning the information war*, 2016

STRATEGICZNE INICJATYWY ROZWOJOWE

Region EŚW przechodzi głębokie zmiany strukturalne w strategicznie istotnych obszarach. Łączy się to z rozwijaniem różnorodnych, wspólnych inicjatyw regionalnych. Proces bardzo dobrze ilustruje budowana od 2016 roku współpraca w ramach tak zwanej inicjatywy Trójmorza[19]. Inicjatywa ta stawia sobie za cel realizację projektów w trzech obszarach: transportu, energetyki oraz cyfryzacji. Trzeci, cyfrowy wymiar nie tylko tworzy osobny zestaw działań, ale także wpływa na dwa poprzednie, stanowiąc niejako serce projektu. Z tego względu odgrywa on ważną rolę w kontekście szans rozwojowych regionu, ale jednocześnie jest szczególnie wrażliwy na współczesne zagrożenia.

Analizując zależności między inicjatywami rozwojowymi a pojawiającymi się ryzykami, zacząć należy od projektów infrastrukturalnych związanych ze wzmacnianiem bezpieczeństwa energetycznego. Jest to kwestia krytyczna w omawianej części Europy. Cechą charakterystyczną regionu jest dominujące przez lata uzależnienie od wschodniego kierunku dostaw surowców takich jak np. gaz ziemny. Tym samym wykorzystywanie surowców energetycznych jako narzędzia walki politycznej mocno zagrażało bezpieczeństwu poszczególnych państw. Po latach trudności związanych z dywersyfikacją źródeł surowców region rozpoczął inwestycje w realizację takich projektów jak budowa korytarzy gazowych Północ–Południe oraz Baltic Pipe. Mają one szansę znacznie przyczynić się do połączenia rynków w regionie, rozwinąć ich konkurencyjność, czyli finalnie umocnić niezależność i bezpieczeństwo energetyczne. Projekty prowadzą do zmiany układu sił politycznych, stawiając sektor energetyczny w pierwszej linii zagrożonych cyberatakami. Niebezpieczeństwo to zmaterializowało się już w ostatnich latach. Świadczy o tym choćby działalność grupy Dragonfly, wykryta i przeanalizowana przez firmę Symantec. Dokonywała ona szeroko zakrojonych operacji cyberszpiegowskich nakierowanych na firmy energetyczne w Europie, w dużej mierze na podmioty z regionu – szczególnie polskie i rumuńskie[20]. Z podobnymi problemami mierzył się także sektor energetyczny krajów bałtyckich[21]. Jak zostało wskazane wcześniej, pozyskiwanie informacji pozwala lepiej rozumieć rywala, poznać jego plany i strategie i dzięki temu budować przewagę konkurencyjną. Jednak warto zauważyć, że zdobyta wiedza może zostać w przyszłości użyta do działań znacznie bardziej poważnych w skutkach. Dzięki poznaniu szczegółów funkcjonowania konkretnych systemów możliwe staje się przygotowanie ataków prowadzących do paraliżu, a nawet fizycznych zniszczeń infrastruktur krytycznych. Należy się spodziewać, że im mocniej państwa regionu budować będą bezpieczeństwo energetyczne, tym bardziej podmioty zainteresowane utrzymaniem strefy wpływów w tym sektorze wykorzystywać będą cyberprzestrzeń do osłabiania tego procesu.

Choć w początkowym okresie wymiar cyfrowej współpracy Trójmorza nie był głównym obszarem działań, z czasem pojawiały się sygnały świadczące o potencjalnym przyspieszeniu. Na szczycie państw Trójmorza w Bukareszcie w 2018 roku zapadła decyzja o umieszczeniu na liście priorytetowych projektów[22] budowy tak zwanej autostrady cyfrowej – Digital 3 Seas Highway (D3SH). W zamierzeniu ma być to infrastruktura cyfrowa

19 Współpraca obejmuje 12 państw: Austrię, Bułgarię, Chorwację, Czechy, Estonię, Litwę, Łotwę, Polskę, Rumunię, Słowację, Słowenię i Węgry.

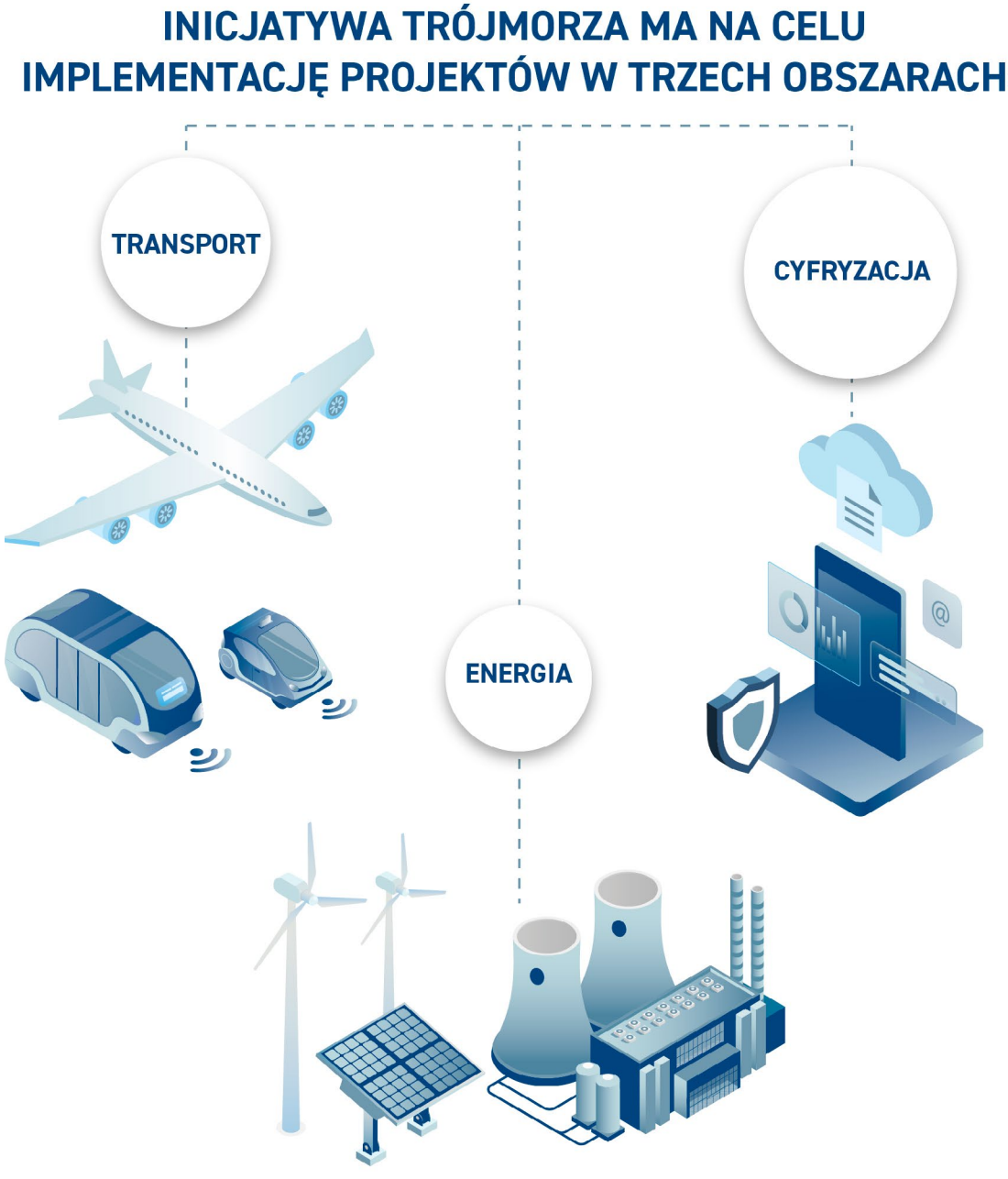
20 Symantec, *Dragonfly: Cyberespionage Attacks Against Energy Suppliers*, 2014, [online]: https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/Dragonfly_Threat_Against_Western_Energy_Suppliers.pdf.

21 Stephen Jewkes, Oleg Vukmanovic, *Suspected Russia-backed hackers target Baltic energy networks*, 2017, [online]: https://www.reuters.com/article/us-baltics-cyber-insight/suspected-russia-backed-hackers-target-baltic-energy-networks-idUSKBN1871W5.

22 Three Seas Initiative Member States, The Three Seas Initiative. Priority Interconnection Projects, 2018 [online]: http://three-seas.eu/wp-content/uploads/2018/09/LIST-OF-PRIORITY-INTERCONNECTION-PROJECTS-2018.pdf.

nowej generacji łącząca cyfrowo – światłowodami i siecią 5G – państwa regionu na osi północ–południe. D3SH to projekt, który umożliwi realizację wielu dalszych strategicznych projektów cyfrowych (np. budowę centrów cyfrowych (*digital innovation hubs*), centrów danych i usług chmurowych, przyspieszenie rozwoju przemysłu 4.0 itd.).

Nie zapadły jeszcze decyzje na temat szczegółów budowy cyfrowej autostrady, jednak do możliwych, i z wielu powodów atrakcyjnych, opcji należy zintegrowanie jej z rozwojem infrastruktury transportowej, konkretnie z projektem Via Carpatia. Via Carpatia jest europejską międzynarodową trasą transportową relacji północ–południe,



mająca połączyć Kłajpedę na Litwie z Salonikami w Grecji. Ze strategicznego punktu widzenia warto byłoby konstrukcję sieci transportowej skoordynować właśnie z budową D3SH. Mogłoby to między innymi umożliwić rozwój transportu przyszłości związanego choćby z autonomicznymi pojazdami, lepsze skomunikowanie i transformację cyfrową regionów. Biorąc pod uwagę strategiczną rolę rozwojową i gospodarczą[23] Via Carpatia, która może zostać jeszcze bardziej wzmocniona dzięki budowie cyfrowej autostrady, należy się spodziewać, że także to przedsięwzięcie potencjalnie stanie się celem wrogich operacji. Tym samym działania z zakresu cyberbezpieczeństwa infrastruktury transportowej i cyfrowej zyskują w regionie jeszcze mocniej na znaczeniu.

REGION EUROPY ŚRODKOWO-WSCHODNIEJ NA MAPIE GEOPOLITYCZNYCH WPŁYWÓW

Region Trójmorza z racji swojego położenia jest krytyczny nie tylko dla graczy z tej części świata. Odgrywa szerszą, ważną rolę na globalnej szachownicy międzynarodowych relacji. Dobrze ilustruje to znaczenie regionu w kontekście rozwijania chińskiej inicjatywy Pasa i Szlaku (ang. *Belt and Road Initiative*, BRI). BRI to strategia Chin zorientowana na globalną ekspansję gospodarczą tego kraju między innymi przez realizację olbrzymich projektów infrastrukturalnych i inwestycyjnych. Przedsięwzięcie ma znaczenie geopolityczne, geoekonomiczne[24], a ważnym jego elementem są działania podejmowane w EŚW, regionie stanowiącym bramę do Europy. BRI zakłada wielosektorowe inicjatywy, przy czym kwestie dotyczące cyfryzacji, zbiorczo nazywane Cyfrowym Jedwabnym Szlakiem (ang. *Digital Silk Road*), odgrywają niezwykle istotną rolę. Stanowią zarówno odrębny obszar działań związany m.in. z masowymi inwestycjami w infrastrukturę cyfrową, jak i czynnik wspierający działania w innych sektorach, np. poprzez tworzenie cyfrowych platform handlowych ułatwiających eksport produktów i usług. Dostrzegając kluczową rolę EŚW w przedsięwzięciu, Chiny stworzyły specjalny format w celu współpracy z krajami regionu, znany powszechnie jako inicjatywa 16+1[25].

Wszystko to pokazuje, że region staje się ważną areną rywalizacji o wpływy między globalnymi, kluczowymi graczami, a wymiar technologiczny tego współzawodnictwa gwałtownie zyskuje na znaczeniu. Obserwowane napięcia dotyczące budowy sieci 5G doskonale ilustrują ten proces. Wraz z ekspansją technologiczną poszczególnych graczy konflikty będą narastać. To kolejny przykład, że decyzje dotyczące cyfryzacji, a także projekty w obszarze cyberbezpieczeństwa zyskują w regionie na znaczeniu zarówno w wymiarze politycznym, jak i strategicznym.

CYBERPRZESTĘPCZOŚĆ

Zagrożenia związane z unikalnymi uwarunkowaniami geopolitycznymi rzutują na specyficzne typy wyzwań, z jakimi mierzą się kraje Trójmorza. Jednak regionu nie omijają także globalne zagrożenia związane z funkcjonowaniem w cyberprzestrzeni. Do najbardziej poważnych należą działania cyberprzestępcze, prowadzące do wielowymiarowych konsekwencji, przede wszystkim coraz poważniejszych strat finansowych. Jak szacuje McAfee i CSIS[26], straty wynikające z cyberprzestępczości mogą sięgać globalnie około 600 miliardów dolarów rocznie. Sam region Europy i Azji Centralnej traci w wyniku tego procesu około 180 miliardów dolarów.

Trójmorze nie jest obszarem wyjątkowym i stanowi zarówno cel działalności cyberprzestępców, jak i teren, z którego prowadzą oni nielegalne działania.

23 A nawet obronną.

24 A także obronne.

25 W chwili obecnej inicjatywa nosi nazwę 17+1 po dołączeniu Grecji.

26 CSIS, McAfee, *Economic Impact of Cybercrime – No Slowing Down*, 2018, [online]: https://www.csis.org/analysis/economic-impact-cybercrime.

Tak jak w przypadku krajów z innych części globu, podmioty z regionu padają ofiarą wielowymiarowych wrogich działań w sieci wykorzystujących na przykład: złośliwe oprogramowanie, ataki phishingowe, spam, DDoS i wiele innych. W ostatnich latach region mocno dotknęły kampanie wykorzystujące oprogramowanie typu ransomware: Wannacry czy szczególnie Bad Rabbit stanowią tu dobre przykłady. Pod względem cyberbezpieczeństwa walka z taką przestępczością jest kluczowa; to zagrożenie przynoszące olbrzymie straty, między innymi społeczne czy finansowe. Państwa regionu nie tylko muszą podnosić poziom cyberbezpieczeństwa, ale także powinny aktywnie zwalczać problem. Szczególnie, że jak wskazuje Europol, niektóre grupy przestępcze w krajach regionu są wyjątkowo aktywne i mają nawet swoje „obszary specjalizacji". Bułgaria i Rumunia na przykład wskazywane są jako kraje, gdzie cyberprzestępcy szczególnie intensywnie trudnią się oszustwami związanymi z płatnościami online[27].

Podsumowując wątek zagrożenia cyberprzestępczością, warto spojrzeć na pewne istotne trendy. Badanie przeprowadzone przez firmę McKinsey wskazuje, że kraje regionu, określane przez autorów mianem *Digital Challengers*, mają wyjątkową szansę, aby przechodząc na wyższy poziom cyfrowej rewolucji, jeszcze mocniej rozwinąć potencjał swoich gospodarek[28]. Jest to niewątpliwie olbrzymia szansa. Jednocześnie warto zauważyć, że cyfryzacja regionu zwiększy jego podatności na zagrożenia ze strony cyberprzestępców, szczególnie tych nastawionych na osiąganie zysków finansowych. Wyzwanie musi być rozpatrywane nie tylko przez pryzmat dobrobytu pojedynczych podmiotów, ale także z punktu widzenia całej gospodarki. By zilustrować problem, warto odwołać się do jednego przykładu – badań przeprowadzonych przez firmę Gallagher. Firma ustaliła, że około 57 000 małych i średnich przedsiębiorstw w Wielkiej Brytanii zbankrutowałoby w tym roku, gdyby padły ofiarą cyberataku uniemożliwiającego im prowadzenie działalności przez mniej niż miesiąc[29]. Biorąc pod uwagę, że przedsiębiorstwa regionu[30] będą coraz mocniej polegać na systemach teleinformatycznych, prowadząc działalność, podobne problemy staną się dla nich równie palące. Jeśli do tego uświadomimy sobie, że zagrożone są nie tylko małe i średnie przedsiębiorstwa, ale także duże podmioty, często z sektorów infrastruktury krytycznej, to problem staje się jeszcze bardziej poważny.

PODSUMOWANIE

Państwa regionu, z racji właściwych sobie uwarunkowań, powinny traktować cyberbezpieczeństwo jako najwyższy priorytet. Rozdział ten skupiał się na czynnikach, które determinują większe ryzyko, inne części publikacji przeanalizują pozytywny potencjał, jaki drzemie w regionie. To właśnie jego wykorzystanie jest kluczowe do tego, aby istniejące trudności móc przekuć w szanse. Aby tak się stało, konieczne jest przede wszystkim uświadomienie sobie, że cyberbezpieczeństwo regionu i poszczególnych krajów warunkuje ich strategiczne cele: rozwój ekonomiczny, bezpieczeństwo narodowe i dobrobyt pojedynczych obywateli. Jako takie wymaga strategicznych, skoordynowanych działań wszystkich krajów i ich międzynarodowych partnerów.

27 Europol, *Internet Organised Crime Threat Assessment*, 2018, s. 67, [online]: https://www.europol.europa.eu/sites/default/files/documents/iocta2018.pdf.

28 McKinsey, *The rise of Digital Challengers*, 2018, [online]: https://digitalchallengers.mckinsey.com.

29 Phil Muncaster, *Over 50,000 UK SMEs Could Collapse Following Cyber-Attack*, 2019, [online]: https://www.infosecurity-magazine.com/news/over-50000-uk-smes-could-collapse.

30 Stanowiące mocno o sile gospodarek poszczególnych państw.

PERSPEKTYWY GOSPODARCZE REGIONU TRÓJMORZA

Rozpad ZSRS w 1991 roku umożliwił krajom Europy Środkowo-Wschodniej inne, w tym horyzontalne, modele integracji międzynarodowej. W latach 2004–2013 większość nowo powstałych lub politycznie uniezależnionych państw stała się członkami Wspólnoty, a następnie Unii Europejskiej. Ogółem państwa regionu stanowią ok. 28% terytorium całej UE, 22% jej populacji, ale wytwarzają tylko ok. 10% jej PKB[31]. Kraje te, jakkolwiek zróżnicowane, mają pewne cechy wspólne i podobne problemy strukturalne. Dwanaście państw członkowskich Trójmorza obejmuje trzy dawne republiki sowieckie, sześć byłych państw przynależących do Paktu Warszawskiego i dwa należące do byłej Jugosławii. Z zachowaniem oczywistych odrębności narodowych, językowych, kulturowych, historycznych i innych, można zauważyć, że wszystkie (poza Austrią) stosowały w przeszłości model gospodarki centralnie sterowanej. Sama Republika Austrii gospodarczo przynależy raczej do zamożnych krajów „Starej Europy", niż wykazuje istotne podobieństwo do pozostałych jedenastu państw Inicjatywy, należy jednak zauważyć, że ma ona historyczne i geograficzne tendencje, jak również gospodarczo-infrastrukturalne interesy, aby w niej uczestniczyć. Pozostałe kraje Europy Środkowo-Wschodniej bywają niekiedy określane jako przynależące do tzw. *emerging markets*, czyli atrakcyjnych dla inwestorów rynków wschodzących, oferujących stosunkowo wysokie zwroty z inwestycji[32].

31 Visegrad Post, *The Three Seas Initiative: Central and Eastern Europe takes charge of its own destiny*, 2016, [online]: https://visegradpost.com/en/2016/08/28/the-three-seas-initiative-central-and-eastern-europe-takes-charge-of-its-own-destiny/.

32 Adam Zaremba, *Quality Investing in CEE Emerging Markets*, *Business, Management and Communication*, 2014, 12(2), s. 176, [online]: https://journals.vgtu.lt/index.php/BME/article/view/3504/2935.

Zgodnie z danymi ośrodka analitycznego SpotData zagregowany PKB państw regionu, wynoszący w 2017 roku 1,7 bln euro, wzrośnie do ok. 2,3 bln euro w 2030[33]. Jednocześnie zbiorczy popyt na szeroko rozumiane inwestycje infrastrukturalne w całym regionie Trójmorza wyniesie nawet ok. 1,15 bln euro do roku 2030, na inwestycje obejmujące drogi, kolej, wodne drogi śródlądowe, porty, lotniska, linie energetyczne i telekomunikacyjne, cyfryzację – nawet ok. 530 mld euro. Same inwestycje infrastrukturalne o znaczeniu transnarodowym mogą pochłonąć do 270 mld euro do roku 2030. Rozwój gospodarczy dwunastu członków Inicjatywy wpisuje się w szerszy kontekst rozwoju Europy Środkowo-Wschodniej jako całego regionu, łącznie z państwami niebędącymi członkami UE, przykładowo krajami Bałkanów Zachodnich.

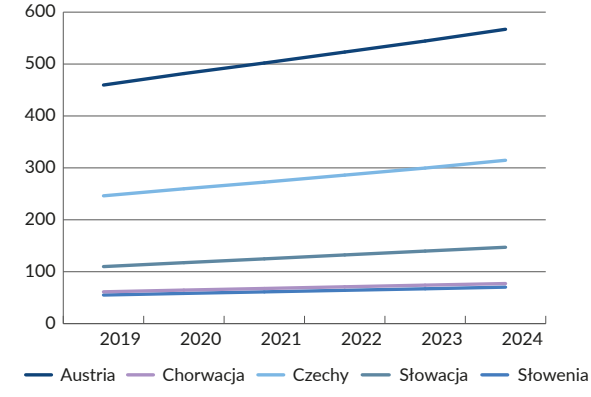
DANE MAKROEKONOMICZNE REGIONU

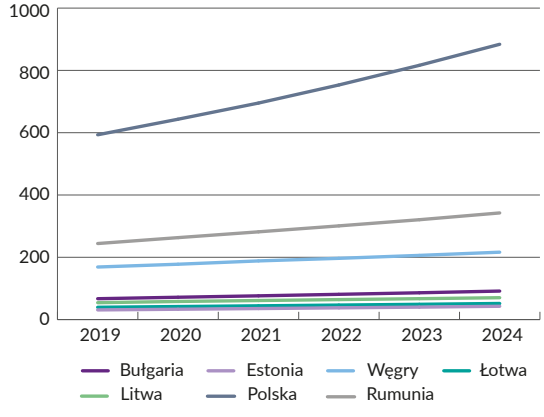
Rozwój gospodarczy państw 3SI można wykazać za pośrednictwem zróżnicowanych wskaźników makroekonomicznych, w tym czterech kluczowych, przedstawiających: zmiany PKB w latach 2019–2024, zmiany PKB *per capita* przy uwzględnieniu parytetu siły nabywczej, zakładane zmiany populacji krajów Inicjatywy oraz udział sektora ICT w PKB i ogóle zatrudnionych[34]. Aby ułatwić przedstawienie danych w formie wykresów liniowych, kraje 3SI podzielone zostały na dwie grupy: grupę A (obejmującą Austrię, Chorwację, Czechy, Słowację i Słowenię) oraz grupę B (obejmującą Bułgarię, Estonię, Węgry, Łotwę, Litwę, Polskę i Rumunię)[35].

A) PKB ORAZ PKB *PER CAPITA*

Zgodnie z prognozą Międzynarodowego Funduszu Walutowego PKB wszystkich państw 3SI w latach 2019–2024 wzrośnie. Najbardziej widoczne jest to na przykładzie dużych gospodarek, takich jak np. Austria, Czechy i Bułgaria. Najmniejszy wzrost osiągnie Estonia i Łotwa (po ok. 12 mld USD), natomiast nominalnie największy odnotuje największa gospodarka – Polska (o ok. 291 mld USD). Średni wzrost PKB w regionie ma wynieść ok. 2,4% w skali roku w latach 2017–2030. Nieco niższą wartość przedstawia OECD, prognozując średni wzrost **o ok. 2%**[36].

Wykres 1 i 2. Wzrost PKB w latach 2019–2024 wśród krajów grupy A (Austrii, Chorwacji, Czech, Słowacji, Słowenii) i B (Bułgarii, Estonii, Węgry, Łotwy, Litwy, Polski i Rumunii) wyrażony w obecnych cenach (w mld USD).





Źródło: IMF, 2019.

33 SpotData, *The Three Seas Initiative & Fund*, 2019, s. 1–7, [online]: http://orka.sejm.gov.pl/opinie8.nsf/nazwa/548_20190314/$file/548_20190314.pdf.

34 Przedostatni wskaźnik obejmuje liczebność populacji zgodnie z przewidywaniami Międzynarodowego Funduszu Walutowego przy uwzględnieniu zmiennej imigracyjnej.

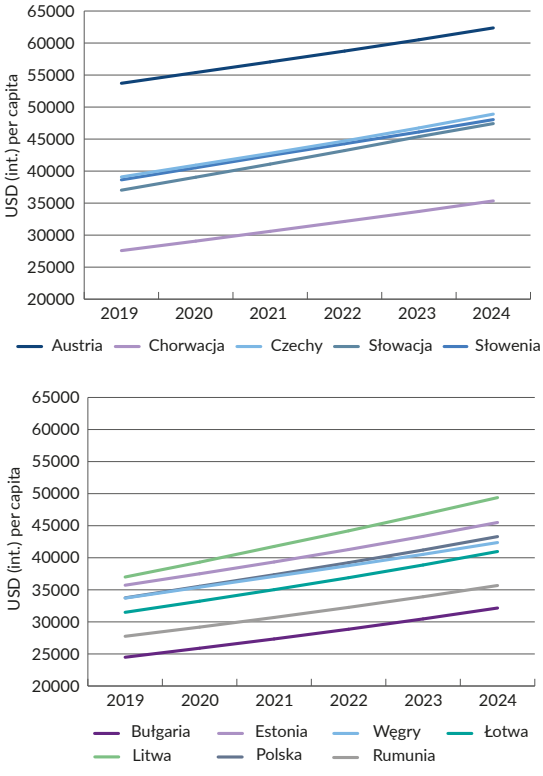
35 Podział ten wynika z zastosowania metody analizy skupień, tzw. metody Warda.

36 Ibidem.

KRAJE REGIONU TRÓJMORZA

Jednocześnie wszystkie kraje 3SI odnotują stabilny wzrost PKB per capita pod względem parytetu siły nabywczej. Największy wzrost ma nastąpić na Litwie (o ok. 12 tys. USD), natomiast najmniejszy – w Bułgarii i Chorwacji (o ok. 7,7 tys. USD).

Wykres 3 i 4. Wzrost PKB per capita w latach 2019–2024 wśród krajów grupy A i B wyrażony w obecnych cenach (w mld USD).

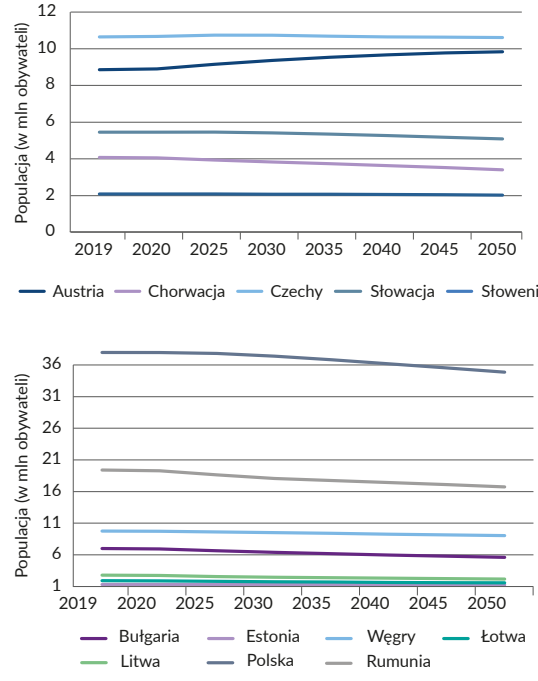


Źródło: IMF, 2019.

B) POPULACJA

Demograficzne prognozy IMF nie są pozytywne dla regionu. Właściwie wszystkie państwa, z wyjątkiem Austrii, odnotują znaczny spadek populacji. Wpisuje się to również w zjawisko starzenia się społeczeństwa, które dotknie kraje 3SI bardziej niż Europy Zachodniej[37]. Oznacza to w praktyce, że podczas gdy kraje 3SI cieszyć się będą znacznym wzrostem gospodarczym, ich kapitał społeczny będzie się zmniejszał. Starzejące się społeczeństwo napotyka również problemy związane z rosnącą grupą relatywnie bardziej ekonomicznie zależnych starszych ludzi przy jednocześnie malejącej grupie relatywnie bardziej innowacyjnych młodszych. Może to pogłębić istniejące już strukturalne problemy niedoinwestowania sektora R&D[38] w regionie Europy Środkowo-Wschodniej.

Wykresy 5 i 6 przedstawiające prognozę zmiany populacji w krajach grup A i B w latach 2019–2050.



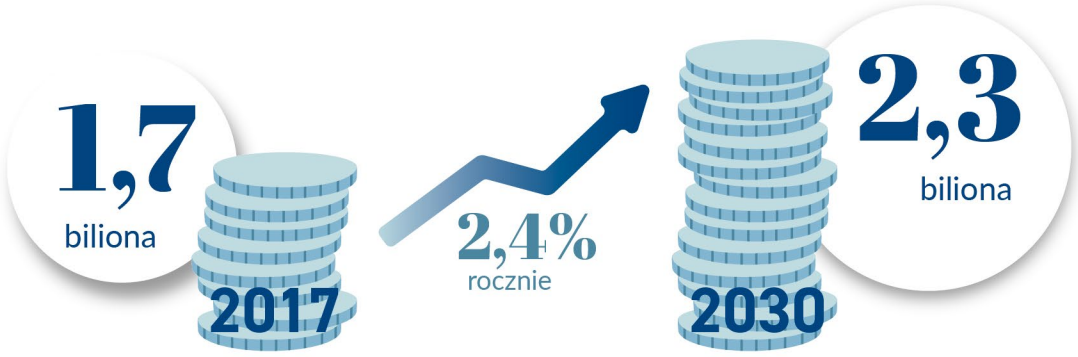
Źródło: IMF, 2019.

Wyzwaniem, któremu region musi sprostać, jest skuteczne przeciwstawianie się hamulcom swojego wzrostu, w tym naświetlonym powyżej problemom malejącej populacji oraz – generalnie – starzejącego się społeczeństwa.

37 Andreas Irmen, Anastasia Litina, *Population Aging and Inventive Activity*, CESifo Working Paper Series no. 5841, 2016, s. 17, [online]: https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2770423_code459177.pdf?abstractid=2770423&mirid=1.

38 Monica Ioana Pop Silaghi, Diana Alexa, Cristina Jude, Cristian Litan, *Do business and public sector research and development expenditures contribute to economic growth in Central and Eastern European Countries? A dynamic panel estimation*, Economic Modelling, 36/2014, s. 108, [online]: http://isiarticles.com/bundles/Article/pre/pdf/17628.pdf.

ZAGREGOWANE PKB REGIONU (w euro)



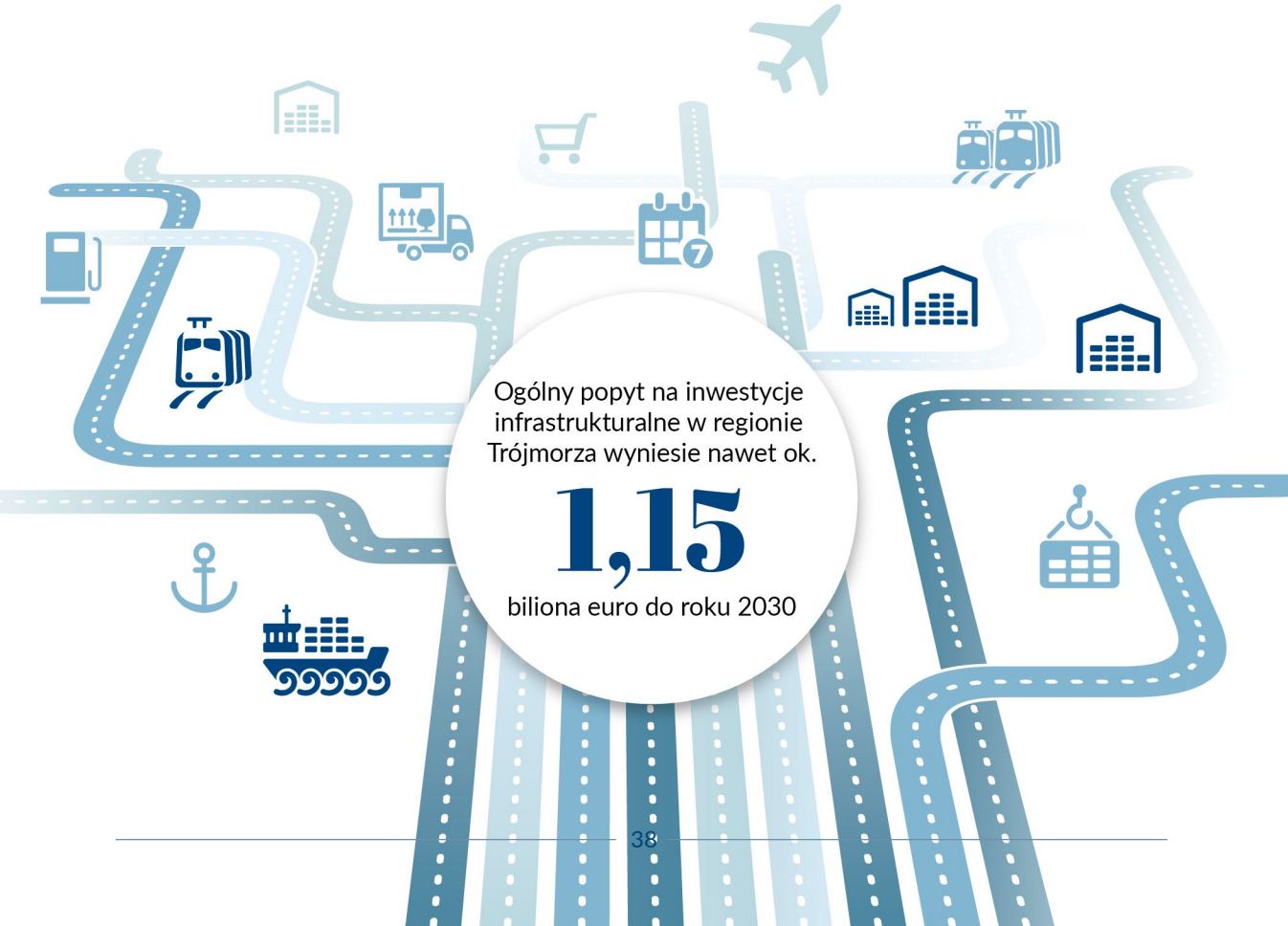


Tabela 1 przedstawiająca dane prognozy demograficznej krajów grup A i B w latach 2019–2050.

Państwa	2019	2020	2025	2030	2035	2040	2045	2050
Czechy	10 649 813	10 674 178	10 742 550	10 738 001	10 687 246	10 648 484	10 634 449	10 611 979
Chorwacja	4 078 848	4 054 406	3 931 639	3 833 236	3 739 478	3 635 856	3 523 223	3 403 390
Austria	8 858 795	8 908 676	9 150 110	9 364 680	9 535 718	9 666 339	9 767 951	9 836 451
Słowenia	2 080 925	2 083 676	2 087 779	2 079 967	2 068 389	2 056 567	2 043 836	2 024 248
Słowacja	5 450 435	5 455 848	5 458 909	5 420 101	5 347 841	5 264 291	5 179 305	5 087 967
Bułgaria	7 000 036	6 943 254	6 659 798	6 402 584	6 182 442	5 979 800	5 791 496	5 605 134
Estonia	1 323 082	1 326 601	1 331 040	1 319 301	1 301 295	1 284 836	1 268 614	1 250 961
Łotwa	1 919 958	1 905 482	1 821 427	1 746 604	1 696 714	1 655 080	1 619 108	1 584 931
Litwa	2 794 204	2 759 230	2 584 736	2 452 166	2 376 255	2 307 089	2 242 358	2 175 738
Węgry	9 757 968	9 739 030	9 634 674	9 520 613	9 396 034	9 271 789	9 158 631	9 041 782
Polska	37 972 841	37 968 244	37 810 482	37 397 916	36 821 234	36 174 048	35 513 097	34 861 135
Rumunia	19 401 655	19 282 488	18 624 968	18 063 702	17 735 220	17 409 228	17 084 433	16 735 514

Źródło: IMF, 2019.

Jedną z prób przezwyciężenia niedoborów krajów 3SI w innowacjach, ale również w transporcie, energii i szeroko pojętej infrastrukturze jest Inicjatywa Trójmorza.

C) SEKTOR ICT

Dane Eurostatu wskazują, że w dynamicznie rosnących gospodarkach państw Trójmorza procentowy stosunek ICT do całości gospodarki niekoniecznie wzrósł na przeciągu pięciu ostatnich notowanych lat (ostatnie dane z 2016), gdyż wartość ta zmalała dla Czech, Estonii, Polski i Słowacji. Udział sektora ICT we wszystkich pozostałych krajach regionu wzrósł. Dane te, w zestawieniu z podnoszącym się udziałem pracowników ICT w danej gospodarce (poza Węgrami), dają ogólny pogląd na rosnące znaczenie sektora w krajach Trójmorza. Pogląd ten znajduje odzwierciedlenie w raporcie *The Digital Three Seas Initiative. Mapping the Challenges to Overcome*, który w szczegółowy sposób przedstawia rozwój gospodarczy regionu. Rosnące zatrudnienie w sektorze ICT odnotowano we wszystkich krajach 3SI[39], przy czym beneficjentem największego wzrostu jest Estonia. Procentowe ujęcie pracowników zatrudnionych w sektorze ICT względem ogółu zatrudnionych wzrosło z wartości 1,9% w 1997 do 4,8% w roku 2017[40].

39 Brak informacji dotyczącej roku 1997 dla Polski.

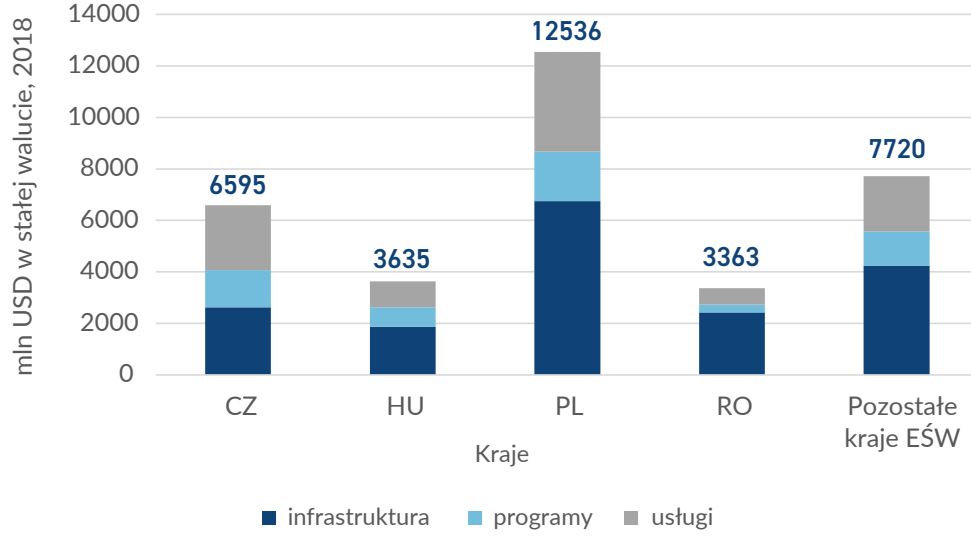
40 Agnieszka Konkel, Marta Przywała (red.). 2018. *The Digital 3 Seas Initiative. Mapping the challenges to overcome*, The Kosciuszko Institute, s. 17, [online]: https://ik.org.pl/wp-content/uploads/digital3seas_initiative_roadmap_report_2018.pdf.

Tabela 2 przedstawiająca wyrażony w procentach stosunek sektora ICT do wytwarzanego PKB dla lat 2011 i 2016 oraz wyrażony w procentach stosunek pracowników zatrudnionych w sektorze ICT względem ogółu zatrudnionych dla lat 2011 i 2016.

	Udział sektora ICT w PKB		Udział pracowników ICT w ogóle zatrudnionych	
	2011	2016	2011	2016
Bułgaria	4,64	5,43	1,89	2,59
Czechy	4,38	4,29	2,79	2,96
Estonia	5,04	4,91	3,33	3,69
Chorwacja	4,05	4,22	1,93	2,34
Łotwa	3,3	4,61	2,15	3,59
Litwa	2,43	2,96	1,88	2,48
Węgry	5,96	5,79	3,69	3,51
Austria	3,25	3,47	2,31	2,55
Polska	3,27	3,22	1,76	2,29
Rumunia	3,1	3,55	1,66	2,27
Słowenia	3,49	3,6	2,34	2,64
Słowacja	4,48	3,99	2,85	3,04

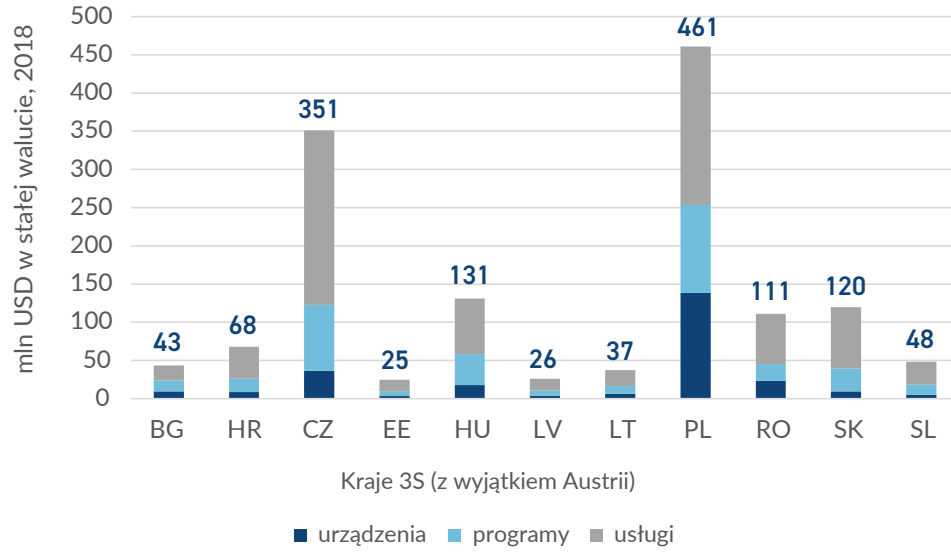
Źródło: Eurostat, 2019.

Wykres 7. Rynek ICT w wybranych krajach 3S.



Źródło: IDC CEMA *Regional Black Book Q418*.

Wykres 8. Rynek cyberbezpieczeństwa 3S.



Źródło: IDC CEMA *Regional Black Book Q418*.

KOMENTARZ EKSPERTA:

Na rynku polskim, największym w regionie, podczas ostatnich kilku lat wzrost inwestycji w zakresie bezpieczeństwa był niebagatelny. Rynek czeski jest jak dotąd najbardziej dojrzały pod względem rozpowszechnienia usług w tej dziedzinie. Organizacje w całym regionie przechodzą właśnie cyfrową transformację, a wdrażając nowe systemy i infrastrukturę, muszą dostosowywać swoje procesy i zabezpieczenia. Dla wielu przedsiębiorstw stanowi to wyzwanie. Przy rosnącej złożoności i powierzchni ataku budżety oraz zasoby są ograniczeniem dla zespołów ds. informatyki i bezpieczeństwa. W rezultacie wiele organizacji zależy od dostawców zabezpieczeń i ich partnerów dystrybucyjnych, chcąc mieć pewność, że rozwiązania w kwestii bezpieczeństwa, w które inwestują, zostały właściwie zastosowane, zoptymalizowane i zintegrowane z istniejącą infrastrukturą.

Chmura ma wszelkie szanse wpłynąć mocno na transformację cyfrową. Firmy niepokoi jednak utrata kontroli nad danymi przy zmianie z infrastruktury lokalnej na chmurę. Problemem jest również złożoność: architektura wielu chmur to także konieczność jej zabezpieczenia. Organizacje rozwijają wielopoziomową strategię, która korzysta z technologii zapewniających bezpieczeństwo i aplikacji, i danych.

Wiktor Markiewicz, IDC Polska, starszy analityk

WYMIAR GOSPODARCZY 3SI

W 2015 roku prezydent Polski, Andrzej Duda, oraz prezydent Chorwacji, Kolinda Grabar-Kitarović, zainicjowali powstanie Inicjatywy Trójmorza jako nieformalnego forum głów państw Europy Środkowo-Wschodniej. Już w 2016 roku w chorwackim Dubrowniku dwunastu członków UE podpisało Wspólną Deklarację określającą cele Inicjatywy. Kluczowym celem Inicjatywy jest stymulacja wzrostu gospodarczego poprzez pogłębienie integracji, a także wzajemne połączenie rynków m.in. poprzez rozwój infrastruktury transportowej, energetycznej i cyfrowej. Rozwój infrastrukturalny zgodny jest z ideą przyświecającą ekonomicznej konwergencji krajów Europy Środkowo-Wschodniej z Zachodnią, przy czym należy zauważyć, że główne wysiłki dotyczące infrastrukturalnego połączenia obydwu regionów od czasów końca zimnej wojny podejmowano przede wszystkim na osi wschód–zachód[41]. W opinii państw Trójmorza nadszedł czas na zrównoważenie tej tendencji poprzez inwestycje na osi północ–południe, co przełożyć się ma na bardziej harmonijny rozwój gospodarczy i zwiększenie międzynarodowego handlu wewnątrzregionalnego. Istotna cecha Inicjatywy to jej oparcie o istniejące mechanizmy europejskie (w tym przede wszystkim politykę spójności i jej instrumenty finansowe), euroatlantyckie i inne, w tym prywatne, źródła finansowania. Oznacza to, że jest ona

41 Polandin, *Explainer: The Three Seas Initiative*, 2019, [online]: https://polandin.com/39043636/explainer-the-three-seas-initiative.

zorientowana również na przyciąganie kapitału zewnętrznego oraz dąży do zintensyfikowania handlu międzynarodowego w ujęciu pozaregionalnym (w tym z Europą Zachodnią i transatlantyckiego). Zasadna wydaje się zatem teza, że plan konwergencji gospodarczej państw 3SI ma charakter wielowymiarowy i holistyczny, co wyróżnia go spośród innych inicjatyw regionalnych, takich jak Grupa Wyszehradzka czy, powiązana z Inicjatywą Jednego Szlaku i Pasa, grupa 17+1.

Infrastrukturalne i gospodarcze wymiary Inicjatywy rozwijały się w konsekwencji szczytów głów państw oraz Wspólnych Deklaracji[42]. Od początku funkcjonowania 3SI miały miejsce cztery szczyty – w Dubrowniku (2016), Warszawie (2017), Bukareszcie (2018) i Lublanie (2019). W ujęciu gospodarczym, już na szczycie w Dubrowniku, państwa 3SI wspólnie wskazały na kluczowe „znaczenie [lepszego wzajemnego] połączenia gospodarek oraz infrastruktury na osi Północ–Południe"[43]. Jednocześnie zwrócono uwagę na rolę regionu 3S w procesie realizacji założeń Jednolitego Rynku Europejskiego, a w związku z tym wagę wykorzystania instrumentów unijnych w rozwoju ekonomicznym Trójmorza, m.in. „Łącząc Europę" (Connecting Europe Facility) oraz innych funduszy inwestycyjnych i infrastrukturalnych. Kolejny szczyt, który odbył się w Warszawie w roku 2017, zapoczątkował organizację 3 Seas Business Forum zrzeszającego przedstawicieli sektora prywatnego. Wskazał tym samym na drugi, poza międzyrządowym, kluczowy wymiar gospodarczej współpracy w ramach inicjatywy Trójmorza. Wspólna Deklaracja z Bukaresztu z roku 2018 podkreśliła z kolei wagę kooperacji pomiędzy organami jednostek samorządu terytorialnego. Jednocześnie z zadowoleniem przyjęto w niej utworzenie Sieci Izb Handlowych Trójmorza.

Opisana dynamika wskazująca na przeniesienie ciężaru rozwoju 3SI z inicjatywy wyłącznie międzyrządowej na samorządy lokalne, regionalne, izby handlowe oraz sektor prywatny wydaje się kluczowa dla możliwości realnego wypracowania wartości dodanej dla gospodarek w ramach prowadzonych projektów 3SI. W tym celu na szczycie w Bukareszcie uchwalono listę szczególnie istotnych projektów połączeniowych (*interconnection projects*[44]). W celu ich współfinansowania przyjęto list intencyjny wskazujący na potrzebę utworzenia osobnego instrumentu finansowego – Funduszu Inwestycyjnego Trójmorza. Ostatni dotychczasowy szczyt, w Lublanie w roku 2019, zakończył się przyjęciem pierwszego raportu dotyczącego rozwoju wspólnych inicjatyw. Raport zawiera sumaryczny przegląd realizowanych projektów z listy priorytetów infrastrukturalnych. Zgodnie z nim wśród realizowanych projektów dominują bilateralne i multilateralne inicjatywy w obszarze transportu międzynarodowego w liczbie odpowiednio 13 i 11 (spośród wszystkich 48 projektów). Uwagę zwraca fakt, że w rozumieniu raportu aż 10 projektów uznawanych jest za przynależące do obszaru infrastruktury cyfrowej, przy czym uwidacznia się znaczna przewaga projektów multilateralnych względem bilateralnych (stosunek 8 do 2). Oznacza to, że kraje regionu są zdecydowanie bardziej zainteresowane wykorzystaniem Inicjatywy Trójmorza do tworzenia wielonarodowych, szerokich projektów regionalnych niż rozwoju infrastruktury w węższej, dwustronnej relacji. Pomimo faktu, że również wśród projektów transportowych i energetycznych podejście wielonarodowe dominuje, w żadnej z tych dwóch dziedzin forma multilateralna nie ma takiej przewagi.

Pozytywna ocena ogólnej liczby zgłoszonych projektów cyfrowych nie utrzymuje się jednak w konfrontacji z danymi o ich statusie, czyli postępie zanotowanym w wykonywaniu projektów. Jedynie cztery

42 Jest to forum nieformalne, wyposażone tylko w pewne elementy zorganizowanej struktury (np. oparcie na *soft law*, utworzenie funduszu, powiązane ciała w postaci Sieci Izb Handlowych).

43 Three Seas Initiative Member States, *The Three Seas Initiative. Priority Interconnection Projects*, 2018, [online]: http://three-seas.eu/wp-content/uploads/2018/09/LIST-OF-PRIORITY-INTERCONNECTION-PROJECTS-2018.pdf.

44 Three Seas Initiative Member States, *The Joint Statement on the Three Seas Initiative (the Dubrovnik Statement)*, 2016, [online]: http://three-seas.eu/wp-content/uploads/2018/06/DUBROVNIK.pdf.

zostały oznaczone jako objęte realnymi działaniami (co prawda niesprecyzowanymi w raporcie), natomiast znaczący postęp miał miejsce tylko w odniesieniu do jednego projektu[45]. Niepokoić może również fakt, że w zasadzie żaden z projektów cyfrowych nie jest uznawany za program flagowy porównywalny do inicjatyw międzynarodowych należących do klasycznej infrastruktury transportowej, takich jak np. międzynarodowa trasa relacji Saloniki–Kłajpeda (Via Carpatia), korytarz bałtycko-adriatycki, czy droga ekspresowa łącząca Tallin z Warszawą (Via Baltica), która wraz z koleją Rail Baltica stworzy transeuropejski korytarz transportowy polepszający połączenie państw bałtyckich z Europą Środkową.

Ostatnim wydarzeniem, które miało miejsce 4 września 2019 r., było podpisanie listu intencyjnego przez prezesów giełd papierów wartościowych Chorwacji, Czech, Węgier, Polski, Rumunii, Słowacji i Słowenii w sprawie powołania wspólnego indeksu giełdowego. Nowy indeks, zwany CEEplus, będzie miał w swoim portfelu ponad 100 spółek pochodzących z partycypujących w nim krajów 3SI. Celem CEEplus będzie zwiększenie atrakcyjności inwestycyjnej regionu, a także harmonizacja współpracy poprzez ułatwienie transgranicznego przepływu inwestycji[46]. Warto zauważyć, że inicjatywa prezesów giełd potwierdza opisaną wyżej tendencję dotyczącą rozwoju instytucjonalno-gospodarczego 3SI wychodzącego poza szczyty głów państw.

PODSUMOWANIE

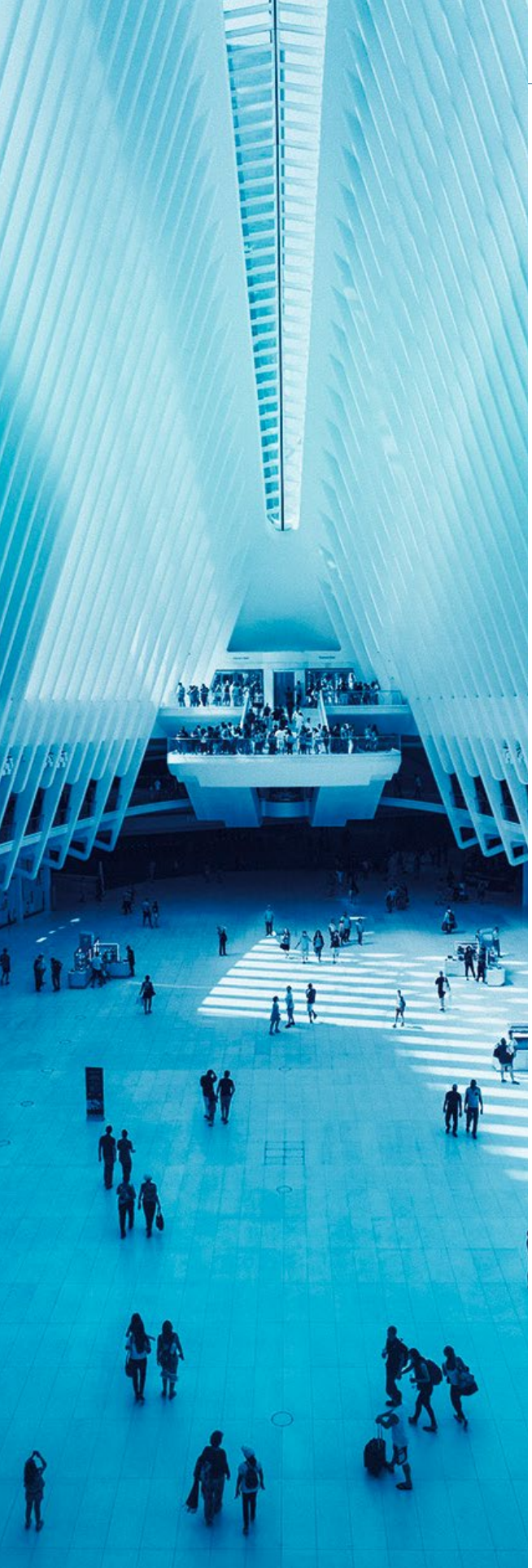
Należące do Europy Środkowo-Wschodniej kraje Unii Europejskiej cechują się jednej strony znacznym potencjałem rozwojowym oraz relatywnie szybko rosnącymi gospodarkami, z drugiej dźwigają bagaż lat niedoinwestowania infrastrukturalnego oraz dominacji połączeń na osi Zachód–Wschód względem osi Północ–Południe. W obliczu sprzyjających warunków politycznych oraz wsparcia polityczno-gospodarczego UE i USA kraje 3SI postanowiły zmaksymalizować integrację regionalną w celu przyspieszenia rozwoju gospodarczego. Zacieśniając współpracę gospodarczej i harmonizując rozwój infrastruktury transportowej, energetycznej i cyfrowej, kraje Inicjatywy Trójmorza dążą do zwiększenia konwergencji z Europą Zachodnią.

Obserwowany od lat 90. XX wieku stabilny i relatywnie szybki wzrost gospodarczy regionu znajduje przełożenie na stopniowe zwiększenie znaczenia i udziału sektora cyfrowego w gospodarkach krajów 3SI. Ma to jednak miejsce w warunkach niekorzystnych zmian demograficznych obejmujących prawie wszystkie z przedmiotowych państw. W obliczu starzejącego się społeczeństwa i malejącego kapitału społecznego szczególnie ważne jest uzyskanie efektu synergii poprzez koordynację działań krajów 3SI, zwiększenie integracji regionu za pomocą stworzenia sieci połączeń infrastrukturalnych oraz, w efekcie, wzmocnienie głosu krajów Inicjatywy Trójmorza na arenach europejskiej i globalnej.

Dynamiczny rozwój Inicjatywy Trójmorza budzi nadzieję, że państwa te w ramach wspólnych działań odniosą się również do innych problemów na poziomie całego regionu, w tym demograficznych. Jest to szczególnie istotne w kontekście zachowania sprzyjających warunków do dalszego szybkiego rozwoju gospodarczego państw 3SI. Na dzień dzisiejszy sama Inicjatywa ułatwiła krajom regionu udowodnienie, że problemom i wyzwaniom przed nim stojącym można stawiać czoła również z własnej perspektywy i inicjatywy, które jednocześnie będą pozytywne i komplementarne wobec szerszego kontekstu integracji europejskiej w ramach UE i wspólnoty transatlantyckiej.

45 Business Forum, *Priority Interconnection Projects*. 2019 Status Report, 2019, s. 1–4, [online]: https://irp-cdn.multiscreensite.com/1805a6e8/files/uploaded/Priority%20Interconnection%20Projects%20-%202019%20Status%20Report.pdf.

46 Forsal.pl, *Powstanie indeks Trójmorza. GPW i 6 giełd regionu szykują CEEplus*, 2019, [online]: https://forsal.pl/finanse/gielda/artykuly/1428603,ceeplus-powstanie-indeks-trojmorza-gpw-i-6-gield-regionu-szykuja-ceeplus.html.



SPOŁECZNE UWARUNKOWANIA POZIOMU CYBERBEZPIECZEŃSTWA PAŃSTW TRÓJMORZA

Niezwykle ważnym ogniwem cyberbezpieczeństwa są ludzie, ich działania, wiedza oraz umiejętności. W niniejszym rozdziale omówione zostaną czynniki społeczne, związane m.in. z edukacją, kapitałem ludzkim czy recepcją nowoczesnych rozwiązań cyfrowych, które determinują obecny i przyszły potencjał cyberbezpieczeństwa dwunastu państw inicjatywy oraz całego regionu Trójmorza (ang. *3 Seas*, 3S). Ze względu na synergiczny charakter inicjatywy względem budowy europejskiego Jednolitego Rynku, w większości przytoczonych statystyk punktem odniesienia jest średnia dla 28 państw Unii Europejskiej.

EDUKACJA

Kraje Trójmorza mierzą się obecnie z procesem dynamicznej cyfryzacji, który przekłada się na konieczność budowy efektywnego systemu cyberbezpieczeństwa w celu zwalczania różnorodnych oraz nieustannie ewoluujących zagrożeń. System ten oprócz ekspertów skupionych w znacznej mierze wokół elementów technicznych obejmuje także zwykłych użytkowników Internetu, których wiedza i umiejętności cyfrowe stanowią praktyczną podstawę bezpieczeństwa sieci.

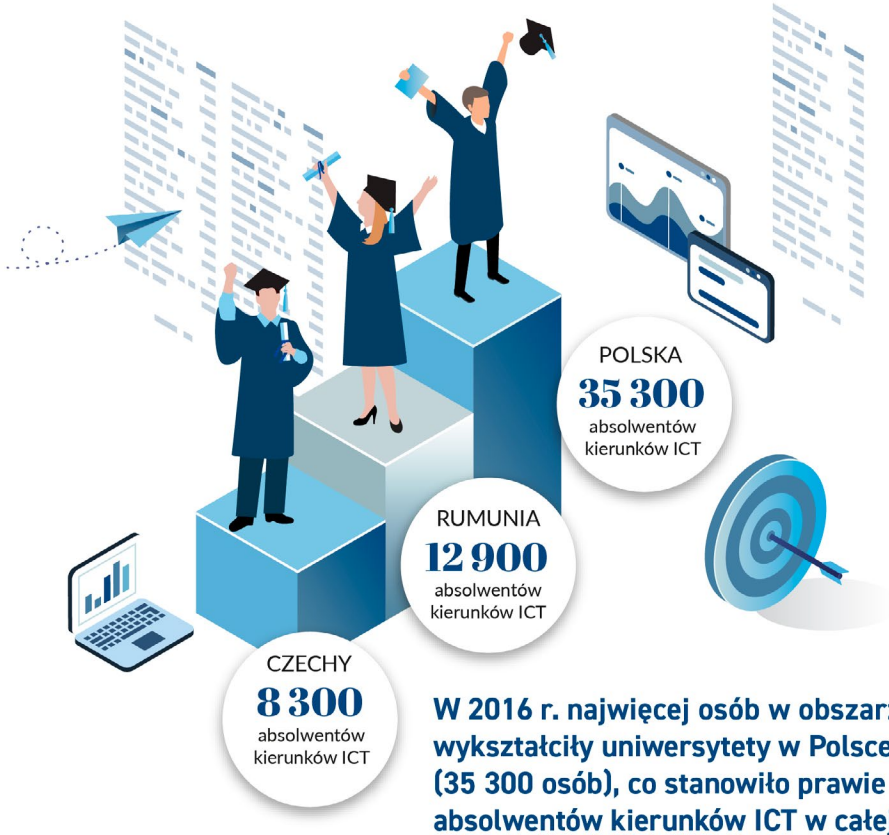
Fakt ten wymusza reformy w zakresie edukacji, która powinna uwzględniać odpowiednie kompetencje cyfrowe na każdym ze szczebli szkolnictwa. Branże zawodowe, nawet te niepokrewne z dziedzinami informatycznymi, również przechodzą lub przejdą cyfrową transformację, przejawiającą się np. wdrażaniem systemu pracy na komputerze czy przechowywania i współdzielenia plików w internetowej chmurze. Aby osiągnąć równowagę pomiędzy inwestycjami w produkcję starego typu a obecnymi wymaganiami rynku,

konieczne jest zapewnienie systemowego wsparcia dla cyfrowej edukacji w postaci przekwalifikowania pracowników oraz kursów dla osób starszych, cyfrowe wykluczenie prowadzi bowiem do wykluczenia społecznego. Z kolei w odpowiedzi na globalny w swym zasięgu problem rynku pracy związany z niedoborem wykwalifikowanych pracowników z umiejętnościami z zakresu nauk ścisłych, technologii, inżynierii i matematyki (ang. *Science*, *Technology*, *Engineering*, *Mathematics*, STEM) należy wspierać w sposób systemowy edukację wystarczającej liczby specjalistów i ekspertów z branży ICT.

Tabela 3. Absolwenci kierunków wyższych (% z ogólnej liczby absolwentów).

PAŃSTWA	EDUKACJA	SZTUKA I HUMANISTYKA	NAUKI SPOŁECZNE, DZIENNIKARSTWO I INFORMACJA, BIZNES, ADMINISTRACJA I PRAWO	NAUKI PRZYRODNICZE, MATEMATYKA I STATYSTYKA, TECHNOLOGIA INFORMACYJNO-KOMUNIKACYJNA (ICT)	INŻYNIERIA, PRODUKCJA I BUDOWNICTWO	ZDROWIE I OPIEKA SPOŁECZNA	USŁUGI	ROLNICTWO, LEŚNICTWO, RYBOŁÓWSTWO I WETERYNARIA	NIEZNANE
UE	9	11	34,1	11	14,8	13,7	3,7	1,7	1,2
Austria	12,2	7,5	33,1	9,8	20,5	7,3	7,8	1,6	0,1
Bułgaria	8,8	7,1	49	6,3	13,4	7,3	6,5	1,7	0
Chorwacja	6	8,9	38,8	9,2	16	9,8	7,2	4	0
Czechy	9,8	8	30,9	9,1	14,9	10,8	6,9	3,2	6,4
Estonia	17,6	12,5	32,8	13,3	14,2	11,7	6,1	1,8	0
Litwa	16,6	9,7	33,2	8,5	14,3	8,3	4,8	3,2	1,3
Łotwa	7,4	7,8	40,3	8	12,6	14,3	7,9	1,9	0
Polska	6,5	8,6	42,1	6,3	17,5	14,2	2,4	2,2	0
Rumunia	13,6	7,2	34,8	7,2	15,6	12,8	7,3	1,5	0
Słowacja	14,2	9,8	37,5	10,6	18,1	10,3	5,5	4	0
Słowenia	13,1	7,5	32,2	8,7	12,4	17,8	6	2,3	0
Węgry	11,2	10,5	34,7	8,1	17	8,4	7,4	2,8	0

Źródło: Eurostat, *Number of tertiary education graduates by field*, 2016.



W 2016 r. najwięcej osób w obszarze ICT wykształciły uniwersytety w Polsce (35 300 osób), co stanowiło prawie 7% absolwentów kierunków ICT w całej Unii i plasuje Polskę na 5. miejscu w UE.

W pierwszym kroku warto w związku z tym prześledzić, na ile szkolnictwo wyższe – kluczowy segment rozwoju gospodarczo-innowacyjnego i procesów digitalizacji – państw Trójmorza odpowiada na problem niedoboru kadry pracowników ICT i STEM i w jakim stosunku do innych kierunków kształci specjalistów z tych dziedzin.

Jak wynika z zaprezentowanych danych, tylko Estonia przewyższa (proporcjonalnie w stosunku do innych kierunków) średnią unijną odsetkiem absolwentów kierunków związanych z umiejętnościami cyfrowymi i sektorem ICT. To właśnie Estonia zatrudnia również największy odsetek specjalistów technologii informacyjno-komunikacyjnych (patrz Tabela 4). Na przeciwległym biegunie znajduje się Bułgaria, Litwa i Polska, które w mniejszym zakresie kształcą ekspertów z zaawansowanymi umiejętnościami informatycznymi. Co ciekawe w tym kontekście, to właśnie w Polsce (37%), na Litwie (40%) i w Bułgarii (42%)[47] najmniejsza liczba przedsiębiorstw zgłaszała w 2017 r. trudności w zatrudnieniu wykwalifikowanych specjalistów, a liczba firm ICT w poszczególnych państwach rośnie (w przeciągu 4 lat 2011–2015 w Bułgarii o 33,6%, w Polsce o 40%, a na Litwie aż o 107,2%). Zaskakująco wysoki wynik osiągnęła natomiast Rumunia, która pomimo rozwiniętego sektora rolnictwa, leśnictwa i rybołówstwa, a także jednego z najniższych odsetków osób posiadających podstawowe umiejętności cyfrowe, kształci po Estonii (proporcjonalnie do innych kierunków) najwięcej specjalistów technologii informacyjno-komunikacyjnych w 3S.

47 Eurostat, *Enterprises that had hard-to-fill vacancies for ICT specialists*, 2017, [online]: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises.

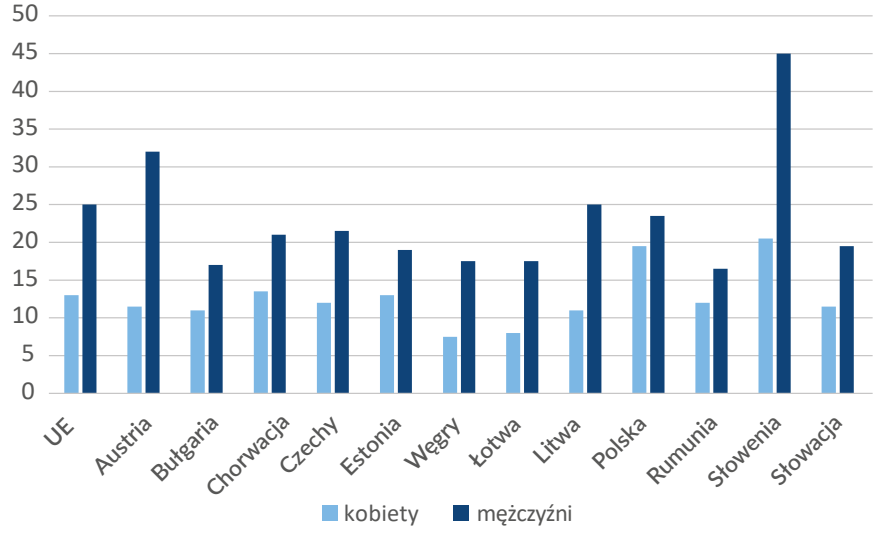
Znacznie korzystniej dla regionu prezentują się statystyki dotyczące odsetka absolwentów kierunków ścisłych takich jak inżynieria, produkcja i budownictwo. Sześć państw Trójmorza dysponuje proporcjonalnie większym odsetkiem ekspertów w tym zakresie niż przeciętne państwo UE. Bardzo wysoki wynik (trzeci najlepszy w UE) zdobyła Austria, która ze względu na swój poziom modernizacji dorównuje państwom Europy Zachodniej i wymyka się generalizacjom dotyczącym regionu (zarówno jeśli chodzi o historię państwa, jak i wskaźniki ekonomiczne).

Powyższe dane pokazują procentowy udział absolwentów kierunków ICT i STEM w całej strukturze absolwentów uczelni wyższych danego państwa. Jeśli przyjrzymy się danym bezwzględnym w tym zakresie, bez procentowego odniesienia do innych informacji, np. liczby wszystkich absolwentów czy populacji, to okaże się, że w 2016 r. najwięcej osób w obszarze teleinformatycznym wykształciły uniwersytety w Polsce (35 300 absolwentów), co stanowiło prawie 7% absolwentów kierunków ICT całej Unii i plasuje Polskę na piątym miejscu w UE.

Polska w rankingu znacznie wyprzedza pozostałe 11 państw regionu, bowiem kolejne państwa o najwyższej liczbie absolwentów to: Rumunia – 12 900, Czechy – 8 300, Austria – 8 200 i Węgry – 5 800. Podobnie prezentują się dane liczbowe absolwentów kierunków STEM: Polska – 76 200 (prawie 11% absolwentów całej UE), Rumunia – 22 100, Austria – 17 100, Czechy – 13 500, Węgry – 9 700.

Warto zwrócić także uwagę, że w ostatnich latach w regionie 3S wzrósł odsetek absolwentów szkół wyższych, którzy ukończyli kierunki STEM. Oprócz wieku ważnym elementem edukacji branżowej jest poszerzanie rynku pracy IT poprzez kształcenie siły roboczej zbalansowanej także pod kątem płci. W Unii Europejskiej w 2016 r. kobiety stanowiły prawie trzy piąte absolwentów szkół wyższych (57,6%)[48]. Warto prześledzić, jak odsetek ten kształtuje się w obrębie kierunków STEM w poszczególnych krajach.

Wykres 9. Różnica w liczbie absolwentek i absolwentów szkół wyższych w dziedzinach STEM (w stosunku do 1000 osób w wieku 20–29 lat).



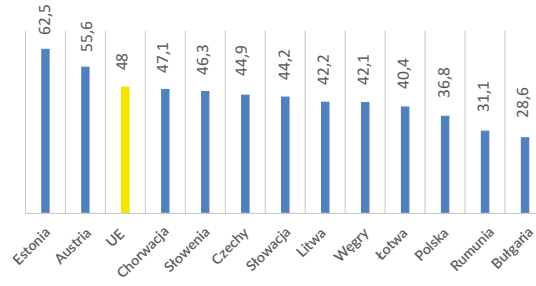
Źródło: Eurostat, *Number of students graduating from tertiary education in science, mathematics, computing, engineering, manufacturing, and construction*, 2016.

48 Eurostat, *Tertiary education statistics*, 2016, [online]: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Tertiary_education_statistics/pl#Udzia.C5.82_m.C4.99.C5.BCczyzn_i_kobiet_w_szkolnictwie_wy.C5.BCszym.

Z powyższych danych wynika, że w UE prawie dwa razy więcej mężczyzn kończyło kierunki STEM w 2016 r., a największą różnicę spośród wszystkich krajów Unii tym zakresie odnotowano w Austrii (ponad 2,5 razy większa liczba absolwentów od absolwentek). W państwach Trójmorza pozytywne dane można było odnotować w Polsce czy w Rumunii, gdzie ok. 40% legitymujących się dyplomem uczelni osób po kierunku STEM to kobiety. Współmierny udział kobiet w sektorze ICT jest ważny, dysproporcja ta uniemożliwia bowiem pełne wykorzystanie potencjału, jaki oferuje branża. Wysiłki na rzecz zachęcenia kobiet do kształcenia się w zakresie nauk ścisłych i promowanie równych szans już od najmłodszych lat mogą nie tylko zniwelować ową różnicę, zbalansować cyfrowy ekosystem, ale stać się również efektywnym sposobem na zmniejszenie deficytu ekspertów z umiejętnościami informatycznymi.

W kontekście edukacji przystającej do potrzeb rynku pracy należy także zwrócić uwagę na wyzwania związane z procesem automatyzacji. Choć obawy dotyczące zastąpienia znacznych rzesz pracowników przez procesy automatyzacji cyfrowej, robotyzacji i sztuczną inteligencję mają swoje uzasadnienie (szacuje się, że do 2025 r. pomniejszą one liczbę miejsc pracy o 75 milionów), to ów postęp technologiczny doprowadzi do wygenerowania zupełnie nowych stanowisk, których technologia przez długi czas nie będzie w stanie zastąpić. Mowa tutaj o zawodach wymagających społecznych umiejętności związanych z zarządzaniem ludźmi czy wdrażaniem wiedzy, na które popyt do 2025 r. wygeneruje ok. 133 milionów nowych miejsc pracy (m.in. *digital cultural commentator*, *ethical technology advocate*, *human body designer*, *IoT data creative*, *personal content creator*, *space tour guide*, *sustainable power innovator*, *freelance biohacker*, *virtual habitat designer*)[49]. Właśnie dlatego architekci państwowych systemów edukacji, także w regionie Trójmorza, w reformach na nadchodzące lata powinni uwzględnić przewidywania dotyczące przyszłości rynku pracy. Analizując programy kształcenia na kierunkach technicznych w krajach 3S, należy wskazać, że wciąż brakuje podejścia interdyscyplinarnego, uwzględniającego realne połączenie wiedzy i umiejętności technicznych z kompetencjami społecznymi. Rozwiązaniem mogą być wprowadzane m.in. na najlepszych uczelniach w USA dyplomy uwzględniające podwójne dziedziny specjalizacji, np. *data science* oraz filozofia, informatyka oraz ekonomia, czy robotyka i psychologia.

Wykres 10. Cyfrowy kapitał ludzki państw 3SI. Procent ogółu populacji o ponadpodstawowych umiejętnościach internetowych.



Źródło: The Digital Economy and Society Index, 2019.

UMIEJĘTNOŚCI CYFROWE

Opracowywany rokrocznie przez Komisję Europejską Indeks Gospodarki Cyfrowej i społeczeństwa Cyfrowego (ang. The Digital Economy and Society Index, DESI) wyznacza miejsca poszczególnych państw UE w osiągniętych postępach w zakresie digitalizacji. Indeks ten kalkulowany jest na podstawie danych statystycznych zagregowanych w pięciu kategoriach. Jedną z nich jest kapitał ludzki (ang. *human capital*), który zgodnie z definicją Komisji mierzy zdolności społeczeństwa niezbędne do rozwoju ogólnego poziomu cyfryzacji państwa za pomocą dwóch kryteriów:

- umiejętności internautów, obliczanych na podstawie liczby oraz złożoności działań dokonywanych przy wykorzystaniu urządzeń cyfrowych i/lub Internetu oraz

49 Agnieszka Konkel, Marta Przywała (red.), *The Digital 3 Seas Initiative. Mapping the challenges to overcome, The Kosciuszko Institute*, 2018, s.39 [online]: https://ik.org.pl/wp-content/uploads/digital3seas_initiative_roadmap_report_2018.pdf.

- zaawansowanych cyfrowych umiejętności i szans rozwoju, rozumianych jako połączenie rezultatów w zakresie poziomu zatrudnienia specjalistów oraz liczby absolwentów sektora ICT[50].

W statystyce DESI za 2019 r. państwa 3SI plasują się w dużej rozpiętości pomiędzy sobą. Krajem Trójmorza, który osiągnął jeden z najlepszych wyników w tym zakresie, nie tylko w regionie, ale także wśród wszystkich państw UE, jest Estonia plasująca się na 4. miejscu, zaś drugim państwem 3SI znajdującym się powyżej unijnej średniej jest Austria (8. pozycja). Dalsza część zestawienia prezentuje się już znacznie mniej optymistycznie i bardzo wyraźnie pokazuje, jak wielkie różnice w kapitale ludzkim dzielą państwa regionu, co obrazuje poniższy wykres. Zgodnie z danymi DESI 2019, Estonia dysponuje ponaddwukrotnie większym kapitałem ludzkim w zakresie cyfryzacji od Bułgarii, która uplasowała się na ostatnim miejscu. Ponadto zaledwie 2 państwa spośród 12 osiągnęły wynik powyżej unijnej średniej, a jak wynika z pełnego indeksu, Rumunia wespół z Bułgarią trafiły na ostatnie miejsca w tej kategorii nie tylko w obrębie państw Trójmorza, ale także całej UE.

Przeciętny obywatel państwa Trójmorza ma bardzo duże braki w wiedzy i kompetencjach, jeżeli chodzi o podstawowe aktywności w sieci. Jak wskazują statystyki Eurostatu, aż 43% populacji UE w 2017 r. nie posiadało wystarczających umiejętności cyfrowych, zaś 17% nie miało ich wcale[51]. Zaledwie dwa kraje 3S znalazły się poniżej średniej unijnej, jeżeli chodzi o liczbę osób deklarujących brak umiejętności cyfrowych lub niekorzystanie z Internetu – Estonia oraz Austria (kolejno 9. i 10. miejsce w zestawieniu dla całej UE), zaś na przeciwległym biegunie znajdują się mieszkańcy Rumunii i Bułgarii (przedostatnie i ostatnie miejsce)[52]. Co ciekawe, zgodnie z danymi Eurostatu z 2011 r., spośród wszystkich państw Trójmorza to właśnie w Bułgarii najmniej pracowników deklarowało wówczas brak wystarczających umiejętności cyfrowych, które pozwoliłyby im na zmianę pracy w przeciągu

Dane przedstawiają wyższy względem średniej UE (37,3%) przeciętny poziom umiejętności cyfrowych obywateli niektórych państw Trójmorza, w tym Austrii (41,2%), Litwy (41,1%), Słowacji (40,5%), Estonii (39,5%) i Słowenii (37,6%).

50 Komisja Europejska, *Human Capital. Digital Inclusion and Skills*, Digital Economy and Society Index Report 2019, s. 7, [online]: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59976.

51 Ibidem, s. 5.

52 Ibidem.

roku[53], a w danych dotyczących liczby użytkowników Internetu wykazujących cyfrowe umiejętności na poziomie podstawowym lub ponadpodstawowym (mierzonym w czterech kategoriach: informacja, komunikacja, tworzenie treści i rozwiązywanie problemów) to w Rumunii i Bułgarii występował ich najniższy odsetek[54]. Wskaźniki te są silnie powiązane z poziomem wykształcenia oraz udziałem rolnictwa w gospodarce państwa – im niższe wykształcenie lub więcej osób zatrudnionych jest w rolnictwie, tym odnotowuje się mniejszą liczbę osób wyedukowanych cyfrowo lub korzystających z Internetu. Warto podkreślić, że Rumunia i Bułgaria to państwa, w których jeden z najbardziej rozwiniętych sektorów zatrudniających najwięcej osób to rolnictwo, leśnictwo i rybołówstwo (w 2017 r. odpowiednio 23,7% i 18,9% ogółu zatrudnionej populacji każdego z państw, podczas gdy średnia unijna wynosi 4,5%). Również w tych dwóch krajach żyje najwięcej osób spośród państw 3S (a w przypadku Bułgarii spośród całej UE), które nigdy nie korzystały z Internetu (odpowiednio 16,1% siły roboczej Bułgarii oraz 12,8% siły roboczej Rumunii)[55].

W państwach Trójmorza, podobnie jak w UE, liczba mężczyzn posiadających przynajmniej podstawowe umiejętności cyfrowe jest większa od liczby kobiet. Wśród użytkowników Internetu kilku państw Unii – Austrii, Estonii, Słowacji, Litwy – posiadanie podstawowych umiejętności cyfrowych jest powszechniejsze niż w uśrednionym społeczeństwie Unii. Dane te odzwierciedlają potencjał państw Trójmorza w obrębie ponadpodstawowych umiejętności cyfrowych, częściej bowiem od uśrednionego obywatela UE (37,3%) wskazana grupa docelowa w Austrii (41,2%), Litwie (41,1%), Słowacji (40,5%), Estonii (39,5%) i Słowenii (37,6%) posiada wyższe kompetencje cyfrowe[56].

Region 3S dysponuje bardzo uzdolnionym zapleczem programistów, którzy od najmłodszych lat kształceni są na niezwykle wysokim poziomie. Jednym z argumentów potwierdzających tę teorię są sukcesy, jakie osiągają reprezentanci krajów Trójmorza w Międzynarodowej Olimpiadzie Informatycznej (ang. *International Olympiad in Informatics*, IOI), corocznym konkursie algorytmiczno-programistycznym dedykowanym uczniom szkół średnich. Zaraz po młodych informatykach z Chin państwem, które wraz z Rosją uplasowało się na drugim miejscu w rankingu IOI obliczanym na podstawie zdobytych medali do 2019 r., była Polska, która zdobyła łącznie 40 złotych, 41 srebrnych i 31 brązowych medali (łącznie 112)[57]. W pierwszej dziesiątce znalazły się również trzy inne państwa regionu inicjatywy: Rumunia (3. miejsce) – 111 medali, Bułgaria (4. miejsce) – 108 medali oraz Słowacja (10. miejsce *ex aequo* z Tajwanem) – 97 medale. Zatem prawie połowa państw światowej dziesiątki kształcącej najbardziej uzdolnionych młodych programistów to kraje Trójmorza. O światowym poziomie polskich programistów świadczy również fakt, że w raporcie Hackers Rank z 2018 r. Polska uplasowała się po Chinach i Rosji na 3. miejscu w rankingu najlepszych programistów. Inne państwa, które również zajęły wysokie miejsca w przytoczonym zestawieniu, to Węgry (5. miejsce), Czechy (9. miejsce), Bułgaria (12. miejsce) oraz Rumunia (20. miejsce).

RYNEK PRACY

Specjaliści ICT są obecnie zatrudniani w każdym sektorze gospodarki. 20% wszystkich firm w Unii Europejskiej w 2018 r. zatrudniało specjalistów

53 Komisja Europejska, *Digital Scoreboard: workers who judge their current ICT skills insufficient for changing job within a year*, 2011, [online]: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators.

54 Komisja Europejska, *Digital Scoreboard: Individuals with basic or above basic digital skills*, 2017, [online]: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators.

55 Komisja Europejska, *Digital Agenda Scoreboard key indicators*, DIGITAL SINGLE MARKET 2018, [online]: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators.

56 Komisja Europejska, *Digital Scoreboard: Digital Skills Indicator- level above basic*, 2017, [online]: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators.

57 International Olympiad in Informatics – Statistics by countries, 2019, [online]: https://stats.ioinformatics.org/countries/.

ICT[58]. Jednocześnie kraje UE zmagają się obecnie z niedoborem pracowników IT – 53% pracodawców w 2018 r. miało problem z ich zatrudnieniem, a co gorsza odsetek ten od 2015 r. systematycznie wzrasta[59]. W całej Unii trudność ta jest najbardziej powszechna w dwóch państwach regionu 3S – Czechach (79%) i Austrii (78%)[60]. Na kolejnych miejscach wśród państw Trójmorza z największą liczbą firm zgłaszających kłopoty w tym zakresie plasuje się Słowenia (65%)[61], Słowacja (60%) i Węgry (60%), a problem ten najrzadziej zgłaszany był w Polsce (37%), na Litwie (40%) i w Bułgarii (42%)[62].

Zgodnie z danymi opublikowanymi przez Eurostat w 2018 r. w regionie EŚW mieliśmy do czynienia ze zwiększonym zatrudnieniem w obrębie sektora informacji i komunikacji, stanowiącym siłę napędową rozwoju cyfrowej gospodarki.

Po raz kolejny warto zwrócić uwagę na przykład Estonii, która jest liderem w zakresie wzrostu zatrudnienia w sektorze ICT, który osiągnął wartość 2,2 punktów procentowych – z 3,5% w 2008 r. do 5,7% w 2018 r. Fakt ten wynika m.in. z istnienia szybkiej oraz nieskomplikowanej procedury założenia działalności gospodarczej w Estonii z wykorzystaniem kanałów online, także przez obywateli innych krajów. Stanowi to przykład bezpośrednich pozytywnych efektów, w tym wypadku także w postaci wpływów podatkowych, wynikających z dostosowania prawa krajowego do wymagań globalnego rynku cyfrowego.

Tabela 4. Zatrudnienie w sektorze informacji i komunikacji (% ogółu zatrudnionych we wszystkich sektorach).

Państwo	2008	2018	różnica
UE	2,8	3,9	1,1
Austria	3,2	4,5	1,3
Bułgaria	1,1	3,0	1,9
Chorwacja	2,2	3,5	1,3
Czechy	4,1	4,1	0
Estonia	3,5	5,7	2,2
Litwa	4,2	3,7	-0,5
Łotwa	1,3	1,7	0,4
Polska	1,9	2,7	0,8
Rumunia	2,8	3,0	0,2
Słowacja	1,9	2,2	0,3
Słowenia	3,3	3,2	-0,1
Węgry	3,6	4,0	0,4

Źródło: Eurostat, *Employed ICT specialist – total*, 2018.

Organizacja Współpracy Gospodarczej i Rozwoju (ang. *Organisation for Economic Co-operation and Development*, OECD) w *Digital Economy Outlook 2017*, raporcie przedstawiającym analizę cyfryzacji gospodarek państw na całym świecie, zbadała poziom zatrudnienia specjalistów ICT. W kontekście wykonywanych obowiązków OECD podzieliła pracowników z sektora telekomunikacji na pięć podstawowych kategorii:

- Managerowie usług ICT (ang. *ICT service managers*),
- Inżynierzy technologii elektrycznych (ang. *electrotechnology engineers*),
- Specjaliści ICT (ang. *ICT professionals*),

58 Eurostat, *ICT specialists - statistics on hard-to-fill vacancies in enterprises*, 2017, [online]: https://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_specialists_-_statistics_on_hard-to-fill_vacancies_in_enterprises#Employment_and_recruitment_of_ICT_specialists.

59 Komisja Europejska, *Digital Scoreboard: Enterprises reporting hard-to-fill vacancies for jobs requiring ICT specialist skills*, 2018, [online]: https://digital-agenda-data.eu/datasets/digital_agenda_scoreboard_key_indicators/indicators.

60 Ibidem.

61 Agnieszka Konkel, Marta Przywała (red.), *The Digital 3 Seas Initiative. Mapping the challenges to overcome, The Kosciuszko Institute*, 2018, s. 33, [online]: https://ik.org.pl/wp-content/uploads/digital3seas_initiative_roadmap_report_2018.pdf.

62 Eurostat, *ICT specialists - statistics on hard-to-fill vacancies in enterprises*, 2017.

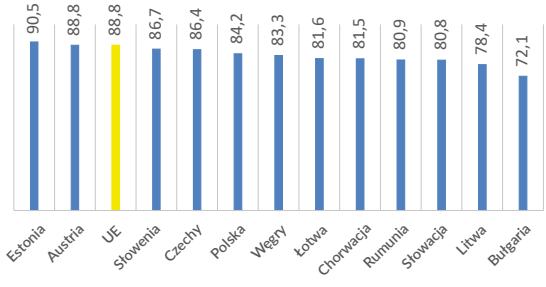
- Technicy ICT (ang. *ICT technicians*),
- Serwisanci obsługi i instalacji sprzętu elektronicznego (ang. *electronics and telecom installers and repairers*).

W większości państw Trójmorza najliczniejszą grupę pracowników stanowią *ICT professionals*, czyli specjaliści prowadzący badania, zapewniający ekspertyzy, testujący i poprawiający funkcjonowanie systemów informatycznych itd., zaś najmniejszą osoby zajmujące się technicznymi aspektami sprzętu telekomunikacyjnego – instalacją, konfiguracją, serwisowaniem.

SPOŁECZNA RECEPCJA DIGITALIZACJI

Ucyfrowienie, mające złożone implikacje dla gospodarki, obejmuje swoim zakresem również przeciętnych obywateli, którzy poprzez łatwość i chęć korzystania z cyfrowych rozwiązań kształtują jego poziom dla całego państwa. Należy prześledzić zatem, w jakim stopniu społeczeństwa 3S adaptują się do świata cyfrowego. Najbardziej podstawowym wskaźnikiem badającym społeczną recepcję procesów związanych z digitalizacją jest dostęp gospodarstw domowych do Internetu, który w państwach Trójmorza prezentuje się następująco:

Wykres 11. Gospodarstwa domowe państw 3SI z dostępem do Internetu (% ogółu gospodarstw domowych).



Źródło: Komisja Europejska, *Digital Agenda Scoreboard key indicators*, 2018.

Do najczęściej wymienianych przez obywateli UE przyczyn nieposiadania dostępu do Internetu należą:

- brak zainteresowania lub potrzeby korzystania z Internetu (46%),
- niewystarczające umiejętności pozwalające na korzystanie z zasobów sieci (43%),
- bariery związane z kosztami (32%).

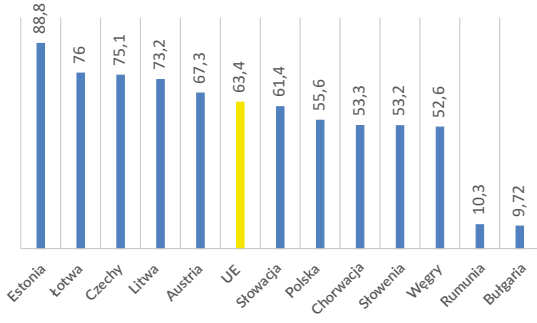
Podane powyżej wyniki procentowe dotyczące częstotliwości pojawiania się danej odpowiedzi są uogólnione dla całej UE, a kolejność powodów jest odmienna w zależności od kraju. Dla przykładu zaledwie 8% Duńczyków wskazało, że posiadanie domowego połączenia internetowego uniemożliwiają im bariery związane z kosztami, podczas gdy tej odpowiedzi w Chorwacji i Bułgarii udzieliło aż 57% respondentów. Z drugiej strony na przestrzeni czterech lat (2013–2017) najbardziej wzrosła liczba osób odpowiadających, że ograniczeniem dostępu do Internetu były dla nich niewystarczające umiejętności cyfrowe (patrz podrozdział *Umiejętności cyfrowe*).

Ciekawie prezentują się wyniki dotyczące udziału ludności regionu Trójmorza w portalach społecznościowych, zgodnie z którymi aż w siedmiu państwach 3SI (kolejno: Węgry, Rumunia, Łotwa, Estonia, Słowacja, Litwa, Chorwacja) przekracza on średnią unijną. Oznacza to, że pomimo niższej liczby gospodarstw domowych posiadających dostęp do Internetu, wyższego odsetka osób, które nigdy z niego nie korzystały, a zwłaszcza niższych umiejętności cyfrowych populacji, w większości państw Trójmorza mamy do czynienia z wysoką partycypacją w mediach społecznościowych (przejawiającą się poprzez m.in. zakładanie kont, wysyłanie wiadomości lub inne aktywności na portalach społecznościowych)[63]. Taka sytuacja rodzi także szereg wyzwań związanych z możliwością niewłaściwego wykorzystania cyberprzestrzeni. Punktem podatnym na manipulacje takie jak rozpowszechnianie fałszywych informacji (ang. *fake news*) bądź ataki socjotechniczne są właśnie osoby o niskich umiejętnościach cyfrowych, które nie znają podstawowych zagrożeń w sieci oraz nie posiadają wiedzy umożliwiającej odpowiednią reakcję w obliczu ataku.

63 Ibidem.

Kolejnym ważnym elementem partycypacji w społeczeństwie cyfrowym jest korzystanie z bankowości internetowej. W przypadku odsetka osób korzystających z bankowości online w krajach 3S jest on wyższy niż unijna średnia w pięciu następujących państwach 3SI: Estonii, Łotwie, Czechach, Litwie oraz Austrii[64]. Po raz kolejny to na ostatnich miejscach plasują się Rumunia i Bułgaria, gdzie z tego rodzaju usług korzystała w 2017 r. 1 na 10 osób (a w niektórych regionach obu państw zaledwie 1 na 50). Trzeba jednak zwrócić uwagę na fakt, że od wyprzedzających je Węgier dzieli te państwa aż odpowiednio 42,3 i 42,88 punktów procentowych. Podobnie duża różnica występuje również w zestawieniu z wszystkimi krajami UE, gdzie do poprzedzającej Grecji Rumunii i Bułgarii brakuje ponad 20 punktów procentowych. Jest to oczywiście bardzo silnie powiązane z plasowaniem się obu państw na ostatnich miejscach w zestawieniu liczby osób posiadających cyfrowe umiejętności, gospodarstw domowych z dostępem do Internetu, czy z wysokim udziałem sektora rolniczego w gospodarce państwa.

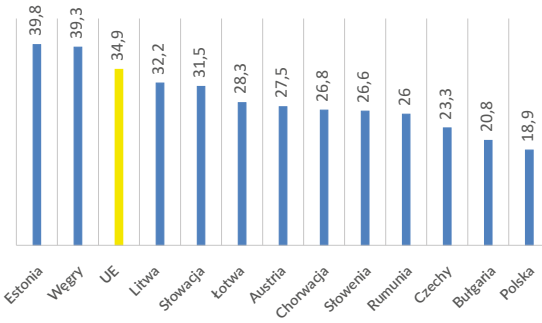
Wykres 12. Korzystanie z bankowości internetowej (% siły roboczej danej populacji).



Źródło: *Komisja Europejska, Digital Agenda Scoreboard key indicators*, 2018.

W kontekście usług chmury obliczeniowej obywatele krajów Trójmorza także w dużo mniejszym stopniu przechowują swoje dokumenty, zdjęcia, muzykę, wideo czy inne pliki w chmurach internetowych od przeciętnego obywatela UE. Zaledwie dwa państwa plasują się powyżej średniej unijnej (oprócz Estonii również Węgry). Co ciekawe narodem 3SI, którego członkowie najrzadziej korzystają z Internetu jako miejsca do przechowywania danych, są Polacy, wypadający też najgorzej w tej kategorii w zestawieniu ze wszystkimi państwami UE[65].

Wykres 13. Przechowywanie plików w Internecie (% siły roboczej danej populacji).



Źródło: Komisja Europejska, *Digital Scoreboard: Used internet storage space to save documents, pictures, music, video or other files*, 2018.

W Unii Europejskiej przechowywanie danych w wirtualnej przestrzeni może doprowadzić do wzrostu wartości rynku chmury z 9,5 mld euro w 2013 r. do 44,8 mld euro w 2020 r., a dostęp do skalowalnej, współdzielonej i elastycznej puli zasobów obliczeniowych radykalnie obniży koszty infrastruktury IT, m.in. sprzętu, danych czy oprogramowania[66]. Konieczne jest zatem zwiększenie adaptacji tej technologii przez kraje Trójmorza, aby optymalizując koszty, doprowadzić do wzrostu konkurencyjności rynku 3S.

Państwa regionu 3S wypadają znacznie lepiej w kontekście korzystania z innej usługi internetowej, jaką jest telefonowanie i wideorozmowa. Większość ich obywateli (z kolejno Łotwy, Bułgarii, Chorwacji, Litwy, Węgier, Estonii, Słowenii i Czech)

64 Ibidem.

65 Ibidem.

66 Agnieszka Konkel, Marta Przywała (red.), *The Digital 3 Seas Initiative. Mapping the challenges to overcome, The Kosciuszko Institute*, 2018, op. cit.

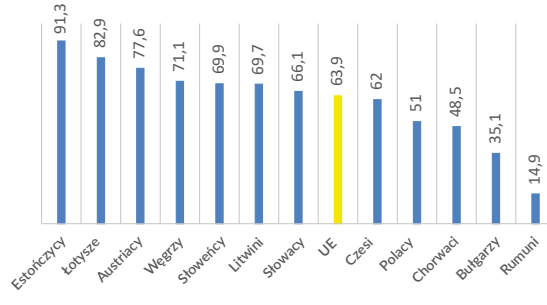
korzysta z tego udogodnienia częściej niż przeciętny obywatel Unii Europejskiej[67]. To fakt zapewne skorelowany z wieloma innymi zmiennymi, jak np. poziomem emigracji, jednak w kontekście prezentowanej analizy niepodważalnym jest, że obywatele państw 3SI korzystają z możliwości, jakie oferują nowoczesne technologie, czasem w wyższym stopniu niż obywatele Europy Zachodniej.

67 Ibidem.

E-GOVERNMENT

W gronie krajów 3S największą liczbę usług e-administracji oferuje Austria, która w całej Unii Europejskiej znajduje się na drugim miejscu. Również obywatele Estonii, Litwy, Łotwy i Słowenii rozwiążą więcej niż unijna średnia kwestii związanych z m.in. rozpoczęciem działalności gospodarczej, obligatoryjnymi czynnościami przy prowadzeniu firmy, formalnościami dotyczącymi utraty i nawiązania stosunku pracy, przeprowadzką, szkolnictwem wyższym, posiadaniem i prowadzeniem samochodu, postępowaniem w sprawie drobnych roszczeń. Poza dostępnością należy również zwrócić uwagę na to, czy obywatele państw Trójmorza faktycznie korzystają z udogodnień oferowanych przez państwowe administracje. W odniesieniu do średniej unijnej, w regionie 3S częściej niż statystyczny Europejczyk z e-usług korzystają kolejno: Estończycy, Łotysze, Austriacy, Węgrzy, Słoweńcy, Litwini oraz Słowacy, co proporcjonalnie pokrywa się z liczbą dostępnych usług e-administracji w danych państwach. Dwa najsłabiej wypadające w tym zestawieniu narody – Bułgarów i Rumunów – dzieli od Estończyków odpowiednio prawie trzykrotnie i ponad sześciokrotnie większy odsetek obywateli załatwiający formalności drogą online.

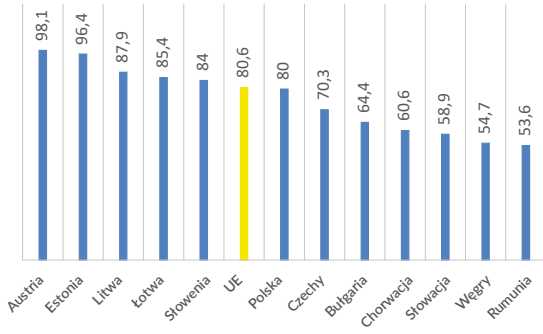
Wykres 14. Dostępność usług e-administracji (w skali 0–100).



Źródło: Komisja Europejska, *Digital Agenda Scoreboard key indicators*, 2018[68].

68 Oryginalne dane pochodzą ze wskaźników *E-Gov Online Service Completion* Komisji Europejskiej zebranych i zestawionych w 2015 r.

Wykres 15. Korzystanie z usług e-administracji (% użytkowników Internetu).



Źródło: Komisja Europejska, *Digital Agenda Scoreboard key indicators*, 2018.

PODSUMOWANIE

Szeroki dostęp do technologii teleinformacyjnych oraz duży kapitał społeczny w zakresie cyfryzacji w oczywisty sposób napędza rozwój produktywności i konkurencyjności regionu. Państwa Trójmorza posiadają w tym zakresie swoje mocne, nawet i wyjątkowe na skalę światową strony, jak i te dystansujące region od państw Europy Zachodniej. Niewątpliwie region wyróżnia kadra bardzo utalentowanych programistów, dynamicznie rozwijający się sektor ICT, który pociąga za sobą bardzo duży wzrost liczby firm ICT oraz zatrudnienia w tej dziedzinie, czy stosunkowo wysoka liczba osób wykształconych w zakresie STEM. Z kolei wyniki, które plasują Trójmorze w ogonie procesów digitalizacji, obejmują znacznie niższą średnią liczbę gospodarstw domowych posiadających dostęp do Internetu, niski kapitał społeczny w zakresie umiejętności cyfrowych czy niewielki udział absolwentów kierunków ICT w ogólnej liczbie osób legitymujących się dyplomem uczelni wyższej.

Powyższe zestawienie danych pozwala wysunąć kilka wniosków:

- Pod względem społecznego potencjału cyfryzacji i cyberbezpieczeństwa kraje 3S są mocno zróżnicowane. Można wyróżnić trzy grupy państw zgodnie z osiąganymi wynikami:
  - I: Austria – najbardziej innowacyjne państwo 3S – i Estonia – lider digitalizacji regionu i jedna z najbardziej zaawansowanych w procesie cyfryzacji gospodarek UE;
  - II: Litwa, Łotwa, Polska, Czechy, Chorwacja, Słowacja, Słowenia, Węgry;
  - III: Bułgaria i Rumunia.
- Choć na przestrzeni ostatnich kilku lat liczba absolwentów kierunków STEM i ICT w państwach 3S wzrasta, to w sytuacji dynamicznie rozwijającego się sektora technologii teleinformatycznych wzrost ten nie jest wystarczająco szybki.
- Niski kapitał społeczny w zakresie umiejętności cyfrowych nie jest jednoznaczny z brakiem utalentowanych specjalistów światowej klasy (przykład Polski, Rumunii i Bułgarii).
- Osiąganie wysokich wyników w kategorii społecznej recepcji cyfryzacji jest pozytywnym trendem, jednak w kontekście niskich umiejętności cyfrowych (w 10 państwach 3SI poniżej średniej unijnej) rodzi obawy dużej podatności na cyberzagrożenia.
- Im większa dostępność usług w zakresie e-administracji, tym większa liczba osób z niej korzystających.
- Niedobór specjalistów z branży ICT i STEM może zmniejszyć wzrost udziału kobiet w sektorze, który będzie miał również pozytywny wpływ na inne aspekty zagadnienia.

ROZWÓJ TECHNOLOGICZNY W REGIONIE TRÓJMORZA

Transformacja cyfrowa gospodarek, która zmienia aktualnie geoekonomiczną mapę świata, stanowi kolejny krok rewolucji informacyjnej obserwowanej od połowy XX wieku. Postęp technologiczny zwiększa wydajność ekonomiczną wielu sektorów, ale przyczynia się równocześnie do obserwowalnego wzrostu zagrożeń. Przykładowo, światowy lider w dziedzinie rozwiązań IT, sieci i cyberbezpieczeństwa w samym tylko roku 2018 zablokował blisko 7 bln zagrożeń[69]. Z jednej strony skala zagrożeń zwiększa się wraz z masowym wdrażaniem najnowszych technologii informacyjnych takich jak AI czy *blockchain*, Internet Rzeczy (IoT) lub 5G. Z drugiej to właśnie rozwój przywołanych technologii jest w stanie dostarczyć nowych rozwiązań i być odpowiedzią na rosnące cyberzagrożenia. Na przykład zdecentralizowany przesył i przechowywanie danych w ramach technologii blockchain może przyczynić się do lepszego zabezpieczenia urządzeń połączonych w ramach IoT[70]. Biorąc pod uwagę fakt, że w 2018 r. ok. 23 mld urządzeń było podłączonych do IoT i narażonych na wykorzystanie w masowych atakach DDoS czy w kontekście cryptominingu, opracowanie nowych rozwiązań w tym zakresie wydaje się koniecznością. Z kolei algorytmy AI już dziś wykorzystywane są do ulepszania zabezpieczeń sieci i systemów poprzez eliminację ich słabych punktów, ale też do automatyzacji ataków wykorzystujących inżynierię społeczną[71].

69 Capgemini Research Institute, *Reinventing Cybersecurity with Artificial Intelligence. The new frontier in digital security*, s. 3, [online]: https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf.

70 Andrew Arnold, *4 Promising Use Cases Of Blockchain In Cybersecurity*, Forbes, 30.01.2019, [online]: https://www.forbes.com/sites/andrewarnold/2019/01/30/4-promising-use-cases-of-blockchain-in-cybersecurity/#742514aa3ac3.

71 BigDataMadeSimple, Why AI is a double-edged sword in the Cybersecurity?, 2019, [online]: https://bigdata-madesimple.com/why-ai-is-a-double-edged-sword-in-the-cybersecurity/.

Podobnie „podwójną naturą" cechuje się rozwój sieci 5G, która zwiększy szybkość i masowość przesyłu danych, jednocześnie tworząc nową jakościowo płaszczyznę ataków dla cyberprzestępców. *Quantum computing* będzie wykorzystywany do łamania algorytmów szyfrujących, na których oparta jest aktualna komunikacja w Internecie (np. RSA), jednak z drugiej strony komunikacja kwantowa umożliwi w pełni bezpieczną wymianę danych w ramach zamkniętego systemu.

Niniejsza analiza prezentuje potencjał technologiczny regionu 3S, uwzględniając pięć wybranych technologii, które w kolejnych dekadach w sposób kluczowy wpływać będą na dynamikę digitalizacji rynków:

- sztuczna inteligencja (AI);
- technologie kwantowe, w tym komputery oraz komunikacja kwantowa;
- blockchain;
- IoT;
- sieć 5G.

SZTUCZNA INTELIGENCJA

Raport *AI in Eastern Europe* na przykładzie m.in. Polski, Litwy, Estonii i Łotwy wskazuje czynniki stanowiące o atrakcyjności inwestycyjnej tych krajów Europy Środkowo-Wschodniej w sektorze AI. Po pierwsze, kraje Trójmorza cechują się bardzo szybkim (w skali globalnej) Internetem – np. Litwa, Estonia i Łotwa znajdują się na liście 23 krajów z najwyższą prędkością (odpowiednio 27,42, 27,91 i 28,63 megabita na sekundę). Po drugie, w krajach EŚW rozwija się przemysł ICT w obszarze AI i powstają startupy zorientowane na wykorzystanie sztucznej inteligencji. Przykładowo w samej tylko Polsce istnieje aż 110 młodych spółek zajmujących się AI, w Estonii 46, na Łotwie 26, na Litwie 29, a w Rumunii – 32[72]. Sztuczną inteligencję w regionie rozwijają również oddziały wielkich globalnych (ale też lokalnych) korporacji, przykładowo w Polsce wdrażaniem AI w ramach technologii finansowych zajmują się Santander Bank Polska czy PKO Bank Polski[73].

Jak wskazują badania, większość startupów branży AI badanych krajów opracowuje przede wszystkim rozwiązania dotyczące rozpoznawania twarzy, wspierania działań marketingowych i przetwarzania maszynowego[74], jednak w regionie wykształca się także specjalizacja na poziomie określonych państw. Przykładowo, w Czechach rozwijają się szczególnie startupy tworzące oprogramowanie na potrzeby cyberbezpieczeństwa, Łotwa specjalizuje się w wykorzystaniu sztucznej inteligencji w technologii finansowej (tzw. fintech), Litwa rozwija sektory e-commerce i gamingowe, Polska słynie z oprogramowania wspomagającego m.in. sektor *life science*, natomiast Rumunia, podobnie jak Litwa i Czechy, rozwija sektory cyberbezpieczeństwa i gier[75]. Wśród państw 3SI środowisko wspomagające rozwój nowoczesnych technologii wspierają obecne w regionie startupy, inkubatory biznesu i parki technologiczne, w tym m.in.: Able, Eleven, Founder Institute (Bułgaria), Innovation Unit, Hubraum, Startup Factory Zagreb, (Chorwacja), InQBay, Point One, Node 5, Prague startup center (Czechy), BuildIt, BioMed Incubator, Climate-KIC (Estonia), Bridge Budapest, Design Terminal, Impact Hub Budapest (Węgry), Commercialization Reactor, TechHub, Startup Wise Guys (Łotwa), StartupHighway, RISE Vilnius, Startup.lt (Litwa), InCredibles, MITEF Poland, ReaktorX (Polska), Central Hub, Cluj-Hub, the Grape (Rumunia), Booster, Eastcubator, CEED Tech (Słowacja), Go:Global, Hekovnik, Geek House (Słowenia)[76].

72 Deep Knowledge Analysis, *AI in Eastern Europe. Artificial Intelligence Industry Landscape Overview 2018*, 2018, s. 11.

73 Rafał Tomaszewski, *Jak banki w Polsce wdrażają sztuczną inteligencję?*, Fintek, 18.03.2019, [online]: https://fintek.pl/jak-banki-w-polsce-wdrazaja-sztuczna-inteligencje-postanowilismy-je-zapytac/.

74 Deep Knowledge Analysis, *AI in Eastern Europe. Artificial Intelligence Industry Landscape Overview 2018*, 2018, s. 11.

75 East-West Digital News, *Startup Investment & Innovation in Emerging Europe. Part 1*, 2018, [online]: http://www.ewdn.com/files/cee_trends.pdf.

76 Ibidem, *Part 4*, s. 55–218, [online]: http://ewdn.com/files/cee_countries.pdf.

Istotne znaczenie mają również inwestycje i subwencje rządowe oparte w wielu przypadkach na narodowych strategiach rozwoju sztucznej inteligencji i obejmujące m.in. system udzielania rządowych dotacji, darmowych porad prawnych, a także innych funduszy i zachęt inwestycyjnych. Przykładowo, Narodowa Strategia Republiki Czeskiej dotycząca Sztucznej Inteligencji zakłada lokalne wsparcie publiczne w przypadku 30% projektów oraz uwzględnia zewnętrzne, publiczne i prywatne, źródła finansowania w wymiarze odpowiednio 23% i 8%. Struktura Strategii obejmuje cele i projekty krótko-, średnio- i długookresowe, których przykładami są:

- stworzenie centrum doskonalenia (*centre of excellence*) z siedzibą w Pradze, które miałoby ściśle współpracować z pozostałymi krajami Grupy Wyszehradzkiej (tj. Polską, Słowacją i Węgrami);
- wielokrotna intensyfikacja aktywności czeskiej w czołowych magazynach badawczych;
- stworzenie z Republiki Czeskiej atrakcyjnego miejsca rozwoju dla światowej klasy badaczy i naukowców z sektora AI do 2035 r.

Wśród obecnie rozwijanych programów badawczych w Czechach do najważniejszych zaliczają się m.in. Nadzieje i Ryzyka Ery Cyfrowej, Pamięć w Erze Cyfrowej, Diagnostyczne Metody i Techniki czy Formy i Funkcje Komunikacji[77]. Na połowę 2019 r. Komisja Europejska wyznaczyła „miękką granicę", zachęcając wszystkie państwa członkowskie UE do stworzenia i opublikowania podobnych narodowych strategii w obszarze AI przed tym terminem. Osiem krajów nie zdążyło ich ogłosić do tego czasu, z czego aż pięć należących do regionu Trójmorza, czyli Austria, Chorwacja, Polska, Słowenia i Węgry[78].

Poza rządami krajowymi rozwój sztucznej inteligencji cieszy się zainteresowaniem organizacji międzynarodowych, w których uczestniczą kraje Trójmorza – UE i OECD. Unia Europejska zakłada, w ramach programu Horyzont 2020, wzrost rocznych inwestycji o 70% i dofinansowanie badań i rozwoju technologii łączną kwotą wynoszącą ok. 1,5 mld euro. Ponadto wspiera łączność i badania nad AI między centrami badawczymi w całej Europie oraz rozwój platformy „AI-on-demand", która ma ułatwić dostęp do rozwiązań AI i premiować ich wykorzystanie w kluczowych sektorach gospodarki. W aspekcie organizacyjnym UE ustanowiła Grupę Roboczą Wysokiego Szczebla ds. AI, która na poziomie eksperckim zajmuje się rozwojem technologii sztucznej inteligencji, w tym również etycznym i nastawionym na spełnianie potrzeb człowieka (tzw. *human-centred*) AI[79]. Podobna inicjatywa przedsięwzięta została na poziomie OECD, które opublikowało zasady etyczne dotyczące rozwoju sztucznej inteligencji. W ich tworzeniu uczestniczyli również przedstawiciele rządów z regionu Trójmorza, w tym Polski, Słowacji i Słowenii. Tworzenie godnej zaufania i opartej na zasadach sztucznej inteligencji przyciąga uwagę organizacji międzynarodowych, które usiłują uniknąć możliwych konfliktów interesów i nadużyć zaufania w relacjach ludzi i maszyn. Szybki rozwój AI może doprowadzić do powstania tzw. osobliwości technologicznej[80] – sytuacji, w której sztuczna inteligencja osiąga poziom rozwoju pozwalający jej na samodoskonalenie niezależnie od jej twórców. Niedostateczny nadzór nad rozbudowanymi systemami sztucznej inteligencji w przyszłości stanowi znaczące ryzyko, które leży u podstaw koncepcji etycznego rozwoju AI.

77 Michal Handl, *The Czech AI Landscape*, Czech Academy of Sciences, s. 13, 2018, [online]: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50809.

78 Peter Teffer, *Eight EU states miss artificial intelligence deadline*, EU Observer, 30.07.2019, [online]: https://euobserver.com/science/145559.

79 High-Level Expert Group on Artificial Intelligence, *Ethics Guidelines for Trustworthy AI*, 2019, [online]: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60419.

80 Amnon Eden, James Moor, *Singularity hypotheses: A Scientific and Philosophical Assessment*, Springer, 2013, s. 1–2, [online]: https://www.researchgate.net/publication/265489594_Singularity_hypotheses_A_scientific_and_philosophical_assessment/link/54da02060cf25013d043a360/download.

Oprócz szans związanych z rozwojem AI istotnym problemem części krajów Trójmorza jest wdrożenie nowości technologicznych z tego zakresu opracowanych przez wysoko wyspecjalizowane ośrodki badawcze i firmy. Przykładowo, raport Digital Poland jako główne przyczyny trudności we wdrażaniu technologii w Polsce wskazuje zarówno niską świadomość klientów dotyczącą tego, jak mogą wykorzystać sztuczną inteligencję dla swoich potrzeb, ale także znaczny deficyt informacyjny w populacji dotyczący samego AI[81]. Wśród innych problemów wymienione są również koszty wdrożeń oraz niewystarczające rozumienie AI wśród personelu i managerów[82]. Trudności z wdrożeniem występują nie tylko w Polsce – jak wskazuje raport McKinsey Global Institute, w rankingu gotowości wdrożeniowej AI również inne kraje regionu Trójmorza (z wyjątkiem Austrii i Estonii) znajdują się poniżej europejskiej średniej lub w dolnym zakresie statystycznym[83].

TECHNOLOGIE KWANTOWE

Technologie kwantowe znajdują się obecnie w momencie przejścia z fazy badawczo-teoretycznej do tworzenia produktów o szerokim, komercyjnym zastosowaniu, takich jak pierwsze komputery kwantowe czy systemy komunikacji wykorzystujące kwantową dystrybucję kluczy kryptograficznych.

W Estonii powstają pierwsze startupy opracowujące software operujący na infrastrukturze komputerów kwantowych. Zajmują się tym takie podmioty, jak Quantastica OÜ (technologie GUI, transkompilacja między kwantowymi językami programowania, połączenia w chmurze) oraz Ketita Labs OÜ (opracowuje hybrydowe algorytmy kwantowo-klasyczne na potrzeby obliczeń kwantowych w najbliższej przyszłości). Na Łotwie promocją *quantum computing* zajmuje się QLatviaSoftware, tworząca struktury zrzeszające badaczy i fascynatów, także z innych państw regionu (grupy istniejące na dzień dzisiejszy: łotewska, węgierska, polska, bałkańska). Funkcjonuje w niej również spółka QuBalt GmbH, która posiada centrum badawcze w Rydze. Prowadzi analizy związane z algorytmami kryptograficznymi odpornymi na technologię kwantową oraz kwantowymi algorytmami oprogramowania. W Polsce informatycy z Centrum Fizyki Teoretycznej Państwowej Akademii Nauk opracowują implementację projektu TEAM-NET, związanego z konstrukcją komputera kwantowego operującego qubitami, czyli bitami kwantowymi[84]. Dodatkowo w ramach polskiej spółki BeIT prowadzone są prace nad wdrożeniem efektywnego algorytmu rozwiązywania problemów NP-zupełnych na komputerach kwantowych[85], natomiast Quantumz.io rozwija Platformę Symulatora Kwantowego (QSP)[86]. W Czechach znajduje się Quantum Phi, specjalizujący się w użyciu technologii kwantowych dla przestrzeni kosmicznej, bezpieczeństwa i przemysłu wojskowego, natomiast w Bułgarii ma swoją siedzibę SHYN, który rozwija teorię wykorzystania algorytmów kwantowych do wizualizacji wariancji (niedokładności) w danych: od cen akcji do prognoz pogody[87].

Technologie kwantowe stanowią jeden z kluczowych priorytetów w ramach agendy innowacyjnej UE. Do pierwszych ważnych impulsów działania należało opracowanie w 2016 roku przez działającą na zlecenie m.in. Komisji Europejskiej międzynarodową grupę ekspertów Manifestu Kwantowego.

81 Digitalpoland, *Map of the Polish AI*, 2019, s. 6, [online]: https://www.digitalpoland.org/assets/reports/map-of-the-polish-ai---2019-edition-i.pdf.

82 Ibidem, s. 21.

83 McKinsey Global Institute, *Notes from the AI Frontier Tackling Europe's Gap in Digital and AI*, s. 40, [online]: https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Artificial%20Intelligence/Tackling%20Europes%20gap%20in%20digital%20and%20AI/MGI-Tackling-Europes-gap-in-digital-and-AI-Feb-2019-vF.ashx.

84 Science in Poland, *Polish contribution to the construction of a quantum computer*, 24.05.2019, [online]: http://scienceinpoland.pap.pl/en/news/news%2C77203%2Cpolish-contribution-construction-quantum-computer.html.

85 BEIT, https://beit.tech/index.html#about_us.

86 Quantum Computing Report, *Private/Startup Companies*, https://quantumcomputingreport.com/players/privatestartup/.

87 Ibidem.

Definiuje on cele w krótkim, średnim i długim okresie, jakie powinna podejmować Unia Europejska, aby uzyskać pozycję jednego z liderów w skali globalnej. Rekomendacje Manifestu posłużyły ustanowionemu przez Komisję w 2017 r. Komitetowi Sterującemu Wysokiego Szczebla do opracowania założeń planu Flagowych Technologii Kwantowych. Obecnie w ramach planu operuje ok 20 platform dotyczących różnych technologii kwantowych, takich jak CiViQ, Quantum Internet Alliance, Uniqorn lub QRANGE[88]. W programy flagowe zaangażowane są również kraje Trójmorza. Przykładowo projekt Uniqorn powstał z inicjatywy austriackiej, CiViQ ma wśród swoich partnerów uniwersytet w Ołomuńcu, natomiast Quantum Internet Alliance jest współtworzony przez uniwersytet w Innsbrucku.

BLOCKCHAIN

Kraje Inicjatywy Trójmorza są bardzo aktywne w sferze wykorzystania technologii *blockchain* przez rodzime startupy. Jako przykład posłużyć mogą chorwackie startupy NodeFactory, Async Labs czy Barrage, czy austriackie spółki innowacyjne takie jak: eloop.to (tokenizujący e-samochody), gridsingularity (działający w sektorze energetycznym), helpar (awangardowy projekt zbudowania ogólnoświatowej pomocy technicznej typu *help desk*) czy Linx4 (zapewniający usługi oparte na blockchain sektorowi bankowości i ubezpieczeń). Oprócz wymienionych na rynku austriackim działają np. Jaroona, Cobra, Trever iQCash-Now, Cryptix, Scytale Ventures, Blacksamanta Capital i wiele innych[89]. Blockchain nie ominął również innych państw regionu – przykładowo estoński Agrello ID jest systemem cyfrowej weryfikacji opartym na łańcuchu bloków, umożliwiającym osobom fizycznym i firmom zawarcie prawnie wiążących umów. Firma oferuje również gotowe szablony do łatwego tworzenia kontraktów różnego typu: B2C, B2B i C2C. Z kolei litewski projekt BitDegree zmienia paradygmat edukacji, wprowadzając nowy sposób uczenia się poprzez stworzenie blockchainowego stypendium w ramach platformy edukacyjnej. Pracodawcy zainteresowani niektórymi obszarami, np. IT, mogą motywować uczniów do rozwijania się w tych kierunkach w celu zaspokojenia potrzeb dynamicznie rozwijającego się rynku pracy[90].

W regionie mają miejsce także ważne wydarzenia, takie jak np. trzydniowy szczyt zorganizowany pod auspicjami rumuńskiego rządu[91] czy konferencja Blocksplit w Chorwacji. Sama Chorwacja należy do awangardy regulacyjnej, ze względu na samorządne unormowanie tej technologii za pośrednictwem Chorwackiego Stowarzyszenia Blockchainu i Kryptowalut (UBIK)[92]. Z kolei Estonia wykorzystuje blockchain w administracji publicznej. Prowadzona przez rząd aplikacja E-stonia umożliwia Estończykom całodzienny dostęp do usług administracji publicznej, przy czym nienaruszalność i bezpieczeństwo systemów oraz danych zapewnione są poprzez wykorzystanie infrastruktury klucza publicznego oraz blockchainu. Dane zabezpieczone są poprzez technologię blockchainowego znakowania czasu (*timestampingu*) oraz przechowywane w zdecentralizowany sposób, również poza granicami państwa[93].

88 Komisja Europejska, *EU funded projects on Quantum Technology*, https://ec.europa.eu/digital-single-market/en/projects-quantum-technology.

89 EnliteAI & Cryptorobby, *Blockchain Landscape Austria*, 2019, [online]: https://www.enlite.ai/works/blockchain-landscape-austria.

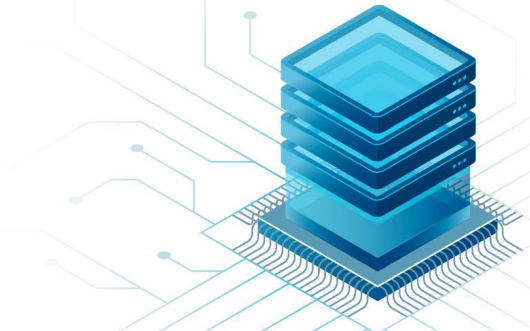
90 Dima Kovalchuk, *Eastern European blockchain projects you should monitor in 2019-2020*, Bitnews Today, 08.07.2019, [online]: https://bitnewstoday.com/news/eastern-europe-an-blockchain-projects-you-should-monitor-in-2019-2020/.

91 Romania Blockchain Summit, https://www.romaniablockchainsummit.com.

92 Molly Jane Zuckerman, *Croatia Launches Self-Regulating Blockchain Organization Amidst Growing Worldwide Trend*, Cointelegraph, 18.02.2018, [online]: https://cointelegraph.com/news/croatia-launches-self-regulating-blockchain-organization-amidst-growing-worldwide-trend.

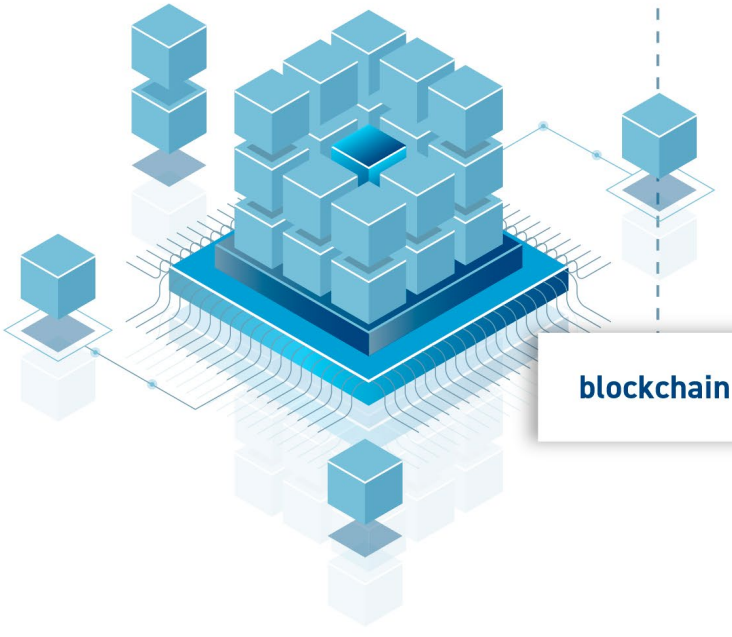
93 Uczelnia Łazarskiego, *Wykorzystanie blockchain przez rząd estoński*, 2019, [online]: https://www.lazarski.pl/pl/wydzialy-i-jednostki/instytuty/wydzial-ekonomii-i-zarzadzania/centrum-technologii-blockchain/wykorzystanie-blockchain-przez-rzad-estonski/ oraz Kersti Kaljulaid, *Estonia is running its country like a tech company*, Quartz, 19.02.2019, [online]: https://qz.com/1535549/living-on-the-blockchain-is-a-game-changer-for-estonian-citizens/.

sztuczna inteligencja



technologie kwantowe, w tym kwantowe komputery i komunikacja

TECHNOLOGIE, KTÓRE WPŁYNĄ NA DYNAMIKĘ CYFRYZACJI RYNKÓW:



blockchain

Internet Rzeczy

sieć 5G

Rozwój rejestrów blockchain znajduje swój wyraz w planowanych przez sektor prywatny inwestycjach. W samym tylko regionie Europy Środkowej w przeprowadzonej przez Deloitte ankiecie prawie 30% pytanych przedstawicieli biznesu zamierza zainwestować lub kontynuować dotychczasowe inwestycje w blockchain na poziomie przynajmniej 100 tys. euro. Respondenci reprezentujący duże firmy planują zainwestować pomiędzy 200 tys. a 2 mln euro w innowacje, przede wszystkim w obszarze zasobów ludzkich[94]. Zainteresowanie rozwojem omawianej technologii wykazuje również Unia Europejska, ponieważ badania i inicjatywy w zakresie praktycznego wykorzystania blockchainu prowadzone są przy wsparciu unijnego obserwatorium i forum blockchainowego[95]. Forum jest przede wszystkim bazą informacji, monitorem oraz hubem informacyjnym na poziomie wspólnotowym, jednak umożliwia też krajom Trójmorza publikację danych o własnych inicjatywach i ułatwia poszukiwanie partnerów (w tym w krajach spoza UE).

INTERNET RZECZY

International Data Corporation (IDC) prognozuje, że kraje regionu EŚW zainwestowały w 2019 r. ponad 11,2 mld USD w sprzęt, oprogramowanie, usługi i łączność IoT, co stanowi ok. 19,5% wzrost względem 2018[96]. Szacuje ponadto, że dochody z IoT w regionie 3S wyniosą ok. 24 mld USD w 2020 roku[97]. Dynamiczny wzrost i rozwój technologii wynika ze znacznego zainteresowania przede wszystkim sektora prywatnego oraz konsumentów. W regionie dostrzegalna jest bardzo silna świadomość znaczenia IoT oraz popyt na te rozwiązania szczególnie na Węgrzech i w Czechach[98], a niektóre źródła wskazują na dobre warunki inwestycyjne także na innych rynkach regionalnych, takich jak Estonia i Polska[99]. W kontekście IoT bardziej niż w przypadku innych technologii region 3S postrzegany jest jako *emerging markets* z tendencją znacznego wzrostu popytu w kolejnych latach.

Uwaga sektora publicznego w kontekście IoT skupia się przede wszystkim na koncepcji czwartej rewolucji przemysłowej (Industry 4.0), czyli wykorzystania nowoczesnej technologii, w tym *machine learning*, *big data* czy AI do stworzenia zintegrowanych środowisk przemysłowych. Środowiska przemysłowego IoT mają być zdolne do znacznie efektywniejszego wykorzystania możliwości związanych z automatyzacją czy też podejmowania trafniejszych decyzji w oparciu o algorytmy wykorzystujące olbrzymie ilości danych (*big data*) oraz komunikację M2M (*machine to machine*). Zintegrowane urządzenia wykorzystane w przestrzeni miejskiej w kontekście stworzenia tzw. *smart cities* cieszą się również wyraźnym zainteresowaniem państw regionu 3S, co znajduje wyraz w umieszczeniu inicjatywy Smart City Forum of the CEE Region na liście priorytetowych programów połączeniowych 3SI. Komplementarną perspektywę obrała Unia Europejska, która w ramach programu Horyzont 2020 w latach 2014–2021 planuje dofinansować rozwój IoT w całej wspólnocie kwotą ok. 500 mln euro. Wśród jej działań harmonizacyjnych wymienić można powstałą w 2016 r. IoT European Platform Initiative. W skład platformy wchodzi siedem flagowych projektów badawczych IoT, spośród których w sześciu znajdują się partnerzy pochodzący z krajów Trójmorza. Są to projekty Inter-IoT, BIG IoT, AGILE, symbIoTe, TagItSmart! oraz VICINITY.

94 Deloitte, *Breaking Blockchain open. Central and Eastern European perspective*, s. 8, 2018, [online]: https://www2.deloitte.com/content/dam/Deloitte/ce/Documents/about-deloitte/ce-blockchain-survey-2018-central-europe-perspective.pdf.

95 EU Blockchain Observatory and Forum, 2019, [online]: https://www.eublockchainforum.eu.

96 Milan Kalal, *The Internet of Things in Central and Eastern Europe – Driving Change, Bringing Opportunity*, IDC, 2016, [online]: https://idctrendspotter.com/internet-of-things-in-cee.

97 Ibidem.

98 Ibidem.

99 World Economic Forum, *Readiness for the Future of Production Report 2018*, 2018, [online]: http://www3.weforum.org/docs/FOP_Readiness_Report_2018.pdf.

SIEĆ 5G

5G to kolejna generacja sieci komórkowych, działająca przy pomocy fal o częstotliwości poniżej 6 gigaherców oraz 20–60 gigaherców i długości kilku milimetrów. Zasadniczo fale wyższych częstotliwości oferują większą przepustowość i mniejsze opóźnienia, ale ograniczony zasięg, ponieważ słabo przenikają przez obiekty, natomiast te poniżej 6 GHz lepiej nadają się do pokrywania bardziej rozległych obszarów. Urządzenia i systemy mobilne korzystające z tych dwóch rodzajów fal tworzą łącznie sieć i technologię 5G[100]. W przeciwieństwie do 4G, które miało jedynie poprawić przepustowość, prędkość wymiany danych, opóźnienia i wykorzystanie spektrum, 5G ma na celu stanowić wsparcie i katalizator przyszłych technologii cyfrowych[101]. Roztoczy przed konsumentami i zainteresowanymi podmiotami przemysłowymi nowe możliwości usług. Umożliwi na przykład przezroczysty dla użytkownika wybór najlepszego połączenia spośród różnorodnych technologii takich jak wi-fi, 4G i łącza radiowe. Będzie ponadto wsparciem dla IoT, dostarczając platformę do połączenia z siecią olbrzymiej liczby obiektów.

Dynamika wdrażania tej sieci jest w krajach Trójmorza rozmaita – od liderów w postaci Austrii i państw bałtyckich przez coraz aktywniejsze Rumunię, Polskę czy Węgry po resztę, goniącą czołówkę. Na Łotwie lokalna sieć telekomunikacyjna Latvijas Mobilais Telefons wygrała jeszcze w roku 2017 przetarg pozwalający na inaugurację sieci 5G w 2020 r. W sierpniu 2018 r. na 5G Techritory, forum państw nadbałtyckich, LMT zaprezentowało zarys bałtyckiej drogi cyfrowej, a we współpracy z Nokią i Intelem wykonało pierwsze testy 5G[102].

Do LMT dołączyli wkrótce inni operatorzy, chociażby TELE2, Bite oraz testujący pierwszy router 5G MikroTik[103]. Łotwie nie ustępuje Litwa, której rynek telekomunikacyjny „należy do najbardziej zaawansowanych w Europie, szczególnie wziąwszy pod uwagę powszechny dostęp do infrastruktury LTE i rozległy ślad światłowodowy”[104], ani Estonia, która uruchomiła swoją sieć nowej generacji już w 2018 r. na skutek współpracy Taltech – tallińskiej politechniki – ze szwedzkimi firmami telekomunikacyjnymi, Telią i Ericssonem[105].

Ericsson podobnie jak Nokia planuje również rozszerzenie inwestycji w Polsce[106], która zamierza (analogicznie jak Węgry) dbać o szybki rozwój infrastruktury obejmującej dostęp do ulepszonego mobilnego internetu szerokopasmowego (eMBB). RP szczególnie zyska na budowie infrastruktury 5G ze względu na rozwinięte zaplecze produkcyjne wielorakich gałęzi przemysłu, w tym rynku telekomunikacji oraz bogatych możliwości dalszego wzrostu, np. w związku z automatyzacją ośrodków bądź procesów produkcji. Jak twierdzi Arun Bansal, wiceprezes Ericssona, operatorzy sieci komórkowych w Polsce dzięki wprowadzaniu łączności 5G na potrzeby przemysłu stoją przed szansą wzrostu przychodów o 40% do roku 2026. Technologia ta wraz z rozwiązaniami poprawiającymi łączność może przynieść gospodarkom Polski i 28 państw członkowskich Unii odpowiednio 67 i 2200 miliardów euro do roku 2030[107].

100 Caitlin McGarry, *What Is 5G? The Definitive Guide to the 5G Network Rollout*, Tom's Guide, 2019, [online]: https://www.tomsguide.com/us/5g-release-date,review-5063.html.

101 Agnieszka Konkel, Marta Przywała (Eds.)., *The Digital 3 Seas Initiative. Mapping the challenges to overcome*, The Kosciuszko Institute, 2018, s. 123, [online]: https://ik.org.pl/wp-content/uploads/digital3seas_initiative_roadmap_report_2018.pdf.

102 LMT, *LMT demonstrates 5G in Latvia for the first time*, 2018, [online]: https://www.lmt.lv/en/press-releases?pid=881.

103 Yi Whan-woo, *Latvia speeds up campaign on 5G, digital technology*, „The Korea Times”, 19.08.2019, [online]: https://www.koreatimes.co.kr/www/nation/2019/08/176_274142.html.

104 BusinessWire, *Lithuania Telecoms, Mobile and Broadband Statistics and Analyses 2019*, 2019, [online]: https://www.businesswire.com/news/home/20190808005746/en/Lithuania-Telecoms-Mobile-Broadband-Statistics-Analyses-2019.

105 ERR.ee, *Telia, Ericsson launch 5G pilot network in Tallinn*, 20.12.2018, [online]: https://news.err.ee/886458/telia-ericsson-launch-5g-pilot-network-in-tallinn.

106 Brianna Clemons, *Ericsson aiming expanding 5G production in Poland*, Markets Morning, 4.09.2019, [online]: https://www.marketsmorning.com/ericsson-aiming-expanding-5g-production-in-poland/.

107 Paweł Rożyński, *Wiceprezes Ericssona: Polska może jeszcze zostać europejskim pionierem w 5G*, „Rzeczpospolita”, 29.08.2019, [online]: https://cyfrowa.rp.pl/opinie/37011-wiceprezes-ericssona-polska-moze-jeszcze-zostac-europejskim-pionierem-w-5g.

Co więcej, Ericsson zatrudnia w Polsce ok. 2400 pracowników, uczestniczących w pracach nad gamą produktów i rozwiązań Ericsson Radio System, czyniąc z Polski jedno z największych centrów B+R w zakresie technologii radiowych[108]. Poza tym przedsiębiorstwem ważnym graczem na rynku lokalnym jest też firma Exatel, planująca w ramach konsorcjum #POLSKIE5G budowę infrastruktury, która obejmie zasięgiem całe państwo[109]. Nie brakuje ponadto inicjatyw lokalnych, omawianą technologię testuje się bowiem obecnie w Warszawie, Łodzi, Zakopanem, Gliwicach oraz Rzeszowie[110]. Operatorzy sieci komórkowych w Czechach mają wprowadzić telefonię 5G do roku 2024, natomiast Słowacja oczekuje działania pierwszej sieci między 2020 a 2022[111]. Ukierunkowane działania dla przyspieszenia rozwoju łącz szerokopasmowych są dla obu tych krajów szczególnie istotne, ponieważ zgodnie z raportem europejskiego obserwatorium 5G wszystkie inne kraje regionu rozwijają lub już testują infrastrukturę piątej generacji[112]. Miastami Trójmorza, w których jest ona szczególnie obecna, są Innsbruck, Tallin, Sofia, Jastrebarsko, Budapeszt, Zalaegerszeg, Ryga, Talsi, Kowno, Wilno, Gliwice, Kraków, Warszawa, Alba Iulia, Cluj-Napoca, Bukareszt oraz Lublana[113]. Niemniej wszystkie kraje Trójmorza pozostają w tyle za pionierem Europy Środkowej, Austrią, która posiada już 25 szerokopasmowych stacji transmisyjnych[114].

Inicjatywy w regionie wspiera działaniami w zakresie 5G Unia Europejska, która zainicjowała stworzenie platformy partnerstwa publiczno-prywatnego, w której biorą udział niektóre państwa Trójmorza, w tym Polska i Słowacja. Ponadto Komisja ogłosiła Plan Działań dot. 5G, wzywający państwa członkowskie do wprowadzenia technologii piątej generacji do roku 2020 oraz wspiera transgraniczne korytarze dla Mobilności Połączonej i Zautomatyzowanej (CAM), współfinansując je m.in. za pośrednictwem Instrumentu „Łącząc Europę". W tym kontekście nader istotne dla regionu wydaje się stworzenie ponadgranicznych „autostrad cyfrowych" korzystających z sieci 5G jako elementów spajających centra przemysłowe Europy Środkowej i Wschodniej.

PRIORYTETOWE PROJEKTY 3SI WYKORZYSTUJĄCE NAJNOWSZE TECHNOLOGIE ICT

Lista programów priorytetowych Inicjatywy Trójmorza zawiera szereg projektów, które w swojej treści i zamierzeniach odnoszą się do omawianych powyżej technologii ICT. Zgłoszony przez Polskę projekt 3 Seas Digital Highway zakłada wykorzystanie m.in. technologii 5G do stworzenia transgranicznej infrastruktury cyfrowej. Do partycypacji zaproszone są wszystkie kraje regionu, a celem projektu jest stworzenie infrastruktury cyfrowej odpornej na cyberataki, umożliwiającej lepszy i bezpieczniejszy transfer danych pomiędzy centrami gospodarczymi 3S. Taka autostrada zakłada również niwelowanie luk w infrastrukturze komunikacyjnej, w tym stojącej za 5G, i ma zapewnić potencjał wzrostu gospodarki danych i transferów z północy na południe[115]. Kolejnym projektem z zakresu nowej generacji sieci mobilnych jest Pilot Project 5G PPDR – Public Protection and Disaster Relief, zgłoszony przez Słowenię, w którym biorą udział również Węgry. Ma on na

108 Ibidem.

109 Marek Jaślan, *Exatel proponuje konsorcjum dla 5G w paśmie 700 MHz*, Telko.in, 12.03.2019, [online]: https://www.telko.in/exatel-zaprasza-do-konsorcjum-5g-w-pasmie-700-mhz.

110 Speedtest.pl, *W Rzeszowie powstanie pierwsza w Polsce publiczna sieć 5G*, 7.07.2019, [online]: https://nowiny24.pl/w-rzeszowie-powstanie-pierwsza-w-polsce-publiczna-siec-5g/ar/c1-14257209.

111 Slovak Spectator, *Slovakia may get 5G network between 2020 and 2022*, 16.11.2017, [online]: https://spectator.sme.sk/c/20698014/slovakia-may-get-5g-network-between-2020-and-2022.html.

112 Komisja Europejska, *5G Observatory Quarterly Report 4*, 2019, s. 23, [online]: http://5gobservatory.eu/wp-content/uploads/2019/07/80082-5G-Observatory-Quarterly-report-4-min.pdf.

113 Ibidem, s. 30–31.

114 Telekom, *Austria is a pioneer country for 5G: T-Mobile Austria launches 5G network*, 26.03.2019, [online]: https://www.telekom.com/en/media/media-information/archive/austria-is-5g-pioneer-country-566746.

115 Three Seas.eu, *The Three Seas Initiative. Priority Interconnection Projects*, 2018, s. 43, [online]: http://three-seas.eu/wp-content/uploads/2018/09/LIST-OF-PRIORITY-INTERCONNECTION-PROJECTS-2018.pdf.

Inicjatywa Cyfrowej Autostrady Trójmorza rozwinięta w ramach Cyfrowej Inicjatywy Trójmorza została na szczycie w Bukarecie włączona do listy strukturalnych projektów priorytetowych.

celu osiągnięcie lepszej sprawności operacyjnej i szybszej reakcji na wypadek sytuacji kryzysowych dzięki innowacyjnemu wykorzystaniu standardowych technologii ICT, w tym sieci 5G oraz IoT[116]. Na liście projektów priorytetowych znalazły się jeszcze dwa projekty, które przewidują w swoich ramach wykorzystanie sieci 5G – jest to chorwacki National Framework Programme for the Development of Broadband Backhaul Infrastructure in Areas Lacking Sufficient Commercial Interest for Investments (NP-BBI Programme). Z kolei w dziedzinie sztucznej inteligencji Węgry zgłosiły projekt Smart City Forum of the CEE Region, w którym partycypują Polska, Czechy, Słowacja, Słowenia, Rumunia, Bułgaria oraz jedno z państw spoza 3S – Serbia. Ma on na celu maksymalizację inwestycji i zwiększenie tempa innowacji w miastach europejskich, między innymi poprzez wdrażanie w tkance miejskiej rozwiązań opartych o AI. Technologie blockchain oraz IoT mają być także wykorzystane w ramach zgłoszonego przez Polskę projektu Centralnoeuropejski Demonstrator Dronów (CEDD), badającego zintegrowane i opłacalne operacje bezzałogowych statków powietrznych, do udziału w którym zaproszone zostały wszystkie kraje Inicjatywy, a także Mołdawia i Ukraina. Głównym celem projektu jest stworzenie środowiska umożliwiającego bezpieczne używanie dronów i wykorzystanie ich potencjału na skalę całej gospodarki.

116 Ibidem, s. 110.

PODSUMOWANIE

Rozwój technologii cyfrowych w państwach Inicjatywy Trójmorza jest dynamiczny, choć trudno zaprzeczyć, że kraje te wciąż pozostają w tym zakresie w tyle za krajami Europy Zachodniej. Sektor cyfrowy w regionie ma znaczny potencjał rozwojowy i mimo niedostatecznych nakładów finansowych na badania i rozwój oferuje dzięki wykwalifikowanej kadrze wiele nowatorskich rozwiązań w obszarze ICT, w tym bezpieczeństwa, jak i może pochwalić się imponującą liczbą start-upów oraz sprzyjającym polityczno-biznesowym klimatem inwestycyjnym.

Ograniczenia w zakresie masowego wdrażania technologii architektury cyfrowej w regionie 3S mogą wynikać z kilku powodów: niektóre technologie są na wczesnym stadium rozwoju komercyjnego (np. *quantum computing*) lub wydają się mniej strategiczne bądź zbyt ryzykowne (np. IoT), szczególnie z punktu widzenia inwestycji publicznych, stanowiących dużą część kapitału przeznaczanego na innowacje w regionie. Deklaracje polityczne w ramach Inicjatywy Trójmorza, szczególnie w kontekście konieczności rozbudowy architektury cyfrowej, wydają się być krokiem w stronę właściwego rozumienia wyzwań leżących przed krajami 3SI i potrzeby pobudzenia innowacyjności. Istnieją zatem przesłanki, że rozwój najnowocześniejszych technologii w regionie odbywać się będzie w kolejnych latach nie tylko w oparciu o jednostkowe inicjatywy spółek startupowych czy ośrodków B+R, ale też zaplanowane działania celowe podejmowane w ramach 3SI lub Jednolitego Rynku Cyfrowego UE.

ROZWÓJ CYBERBEZPIECZEŃSTWA W REGIONIE TRÓJMORZA Z PERSPEKTYWY PRAWNEJ

Przejrzyste przepisy i regulacje stanowią czynnik kluczowy dla przedsiębiorstw przy decyzjach o działaniu i rozwijaniu aktywności w danym kraju. Zapewniając określony poziom stabilności, a zatem i możliwości utrzymania firmy, zajmują także centralne miejsce w ochronie praw przedsiębiorstw i zapewnianiu odpowiedniego poziomu bezpieczeństwa wobec korupcji czy konieczności dochodzenia praw przed sądem. Cyberbezpieczeństwo wyłoniło się jako kwestia prawna dopiero od niedawna, dlatego stan legislacji go dotyczącej w państwach Europy Środkowej i Wschodniej w dużym stopniu zależy od UE, gdzie odpowiednie przepisy przyjęto w ostatnich latach. Uważne przyjrzenie się trzem głównym regulacjom UE w dziedzinie cyberbezpieczeństwa może okazać się użyteczne w rozważaniach nad stopniem zaawansowania i zaangażowania krajów EŚW w tej kwestii. Inne narodowe i ponadnarodowe inicjatywy nielegislacyjne również stanowią istotne narzędzia podkreślające zdecydowane działania państw w sprawie cyberbezpieczeństwa. W dobie rosnącej globalizacji powiązań handlowych i biznesowych spójność oraz ujednolicenie różnorodnych krajowych i regionalnych regulacji prawnych także nosi znamiona elementu o bardzo korzystnym charakterze.

NARODOWE SYSTEMY CYBERBEZPIECZEŃSTWA W EŚW – IMPLEMENTACJA DYREKTYWY NIS

W ujęciu chronologicznym dyrektywę na rzecz bezpieczeństwa sieci i systemów informatycznych (NIS)[117] przyjęto jako pierwszą na terenie całego

117 Parlament Europejski i Rada (UE), *Dyrektywa 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii*, Dz. U. UE L 194, s. 1–30, 19 lipca 2016.

RODO ustanowiła wspólne normy prawne ochrony danych dla wszystkich przedsiębiorstw działających w UE. Jej cel jest dwojaki: przede wszystkim zapewnia ochronę danych osobowych obywateli UE, ale także gwarantuje swobodę przepływu danych między Państwami Członkowskimi – co jest szczególnie istotne dla przedsiębiorstw działających na globalnym rynku.

obszaru Trójmorza zgodnie z celami ogłoszonymi w unijnej strategii cyberbezpieczeństwa z roku 2013[118]. To pierwsza regulacja ogólnounijna dotycząca cyberbezpieczeństwa. Mając na celu osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych, wspiera rozwój krajowych zdolności w cyberprzestrzeni, usprawnienie międzypaństwowej współpracy na tym polu oraz wnikliwy nadzór sektorów o krytycznym znaczeniu dla każdego kraju. Na potrzeby ostatniego z tych celów dyrektywa wyznacza dalekosiężne powinności i wymagania operatorom usług kluczowych (OUK)[119] oraz dostawcom usług cyfrowych (DUC)[120], pozwala jednak państwom członkowskim ustalać, które podmioty spełniają kryteria OUK. Wiele odsłania uważniejsze spojrzenie na szczegóły przeniesienia dyrektywy NIS do prawodawstwa poszczególnych państw, w dużej mierze odbijające ich wizję i ambicje osiągnięcia celów w niej nakreślonych. Po pierwsze warto zauważyć, że – nie licząc trzech państw (Rumunii, Bułgarii i Węgier) – wszystkie kraje Trójmorza skorzystały przy transpozycji dyrektywy z okazji dodania sektorów definiowanych jako OUK, poddając je zatem surowszemu nadzorowi pod względem cyberbezpieczeństwa (patrz tabela 1). Szczególnie dobrze obrazuje to przykład państw bałtyckich, wśród których Estonia dopisała do listy OUK wszystkie sektory komunikacji i identyfikacji elektronicznej, Łotwa dołączyła prawodawstwo i wymogi odnoszące się do infrastruktury bankowej i finansowej, a Litwa włączyła kilka branż, w tym obronę cywilną i narodową.

Tabela 5. Branże dołączone w poszczególnych państwach do listy operatorów usług kluczowych objętych dyrektywą NIS.

Państwo	Addition(s)
Austria	• administracja publiczna
Bułgaria	brak
Chorwacja	• dodatkowa infrastruktura cyfrowa
Czechy	• dodatkowa infrastruktura cyfrowa • przemysł chemiczny
Estonia	• dostawcy usług komunikacji elektronicznej • media publiczne • dostawcy usług identyfikacji cyfrowej i podpisów cyfrowych • dostawcy usług ciepłowniczych
Litwa	• działalność przemysłowa • branża chemiczna i jądrowa • administracja państwowa • obrona cywilna • działalność związana ze środowiskiem • obrona narodowa • polityka zagraniczna i bezpieczeństwo
Łotwa	• bankowość i infrastruktura rynków finansowych podlegają prawodawstwu i wymogom sektorowym
Polska	• energetyka i ciepłownictwo • górnictwo i wydobycie
Rumunia	brak
Słowacja	• przemysł farmaceutyczny i chemiczny • administracja publiczna • komunikacja elektroniczna • usługi pocztowe
Słowenia	• branża ochrony środowiska
Węgry	brak

Źródło: ECSO i DIGITALEUROPE, śledzenie implementacji NIS[121]

118 *Wspólny komunikat do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*, 7 lutego 2013.

119 Operator usług kluczowych oznacza podmiot publiczny lub prywatny o istotnej roli w zapewnianiu bezpieczeństwa w dziedzinie służby zdrowia, energetyki, transportu, bankowości, infrastruktury rynków finansowych, zaopatrzenia w wodę pitną. Zob. art. 5 ust. 2 oraz załącznik II dyrektywy NIS.

120 Zgodnie z artykułem 4 (definicja 6) dyrektywy NIS „dostawca usług cyfrowych" oznacza każdą osobę prawną, która świadczy usługi cyfrowe.

121 ECS and DIGITALEUROPE, NIS Implementation Tracker, 2019, [online]: https://www.digitaleurope.org/resources/nis-implementation-tracker/.

Sektory objęte definicją OUK w dyrektywie NIS: energetyka, transport, bankowość, infrastruktura rynków finansowych, służba zdrowia, zaopatrzenie w wodę pitną i jej dystrybucja, pewne podmioty infrastruktury cyfrowej (punkty wymiany ruchu internetowego, dostawcy usług DNS, tj. systemu nazw domen, oraz zarządzający rejestracją nazw domen najwyższego poziomu, tj. TLD).

W efekcie stan bezpieczeństwa informacji i sieci w EŚW jest względnie jednolity – jak oczekiwano pod dyrektywie NIS. Dodatkowo państwa Trójmorza z reguły obejmują ochroną większą liczbę sektorów niż reszta Unii. Elastyczne definicje OUK umożliwiły części z nich ustanowienie ściślejszego nadzoru branż bardziej podatnych na cyberataki, wzmacniając tym samym poziom ochrony.

ZABEZPIECZANIE DANYCH W ERZE INFORMACJI – ROZPORZĄDZENIE RODO

Drugą podstawą europejskiego prawodawstwa w kwestii cyberbezpieczeństwa, a dokładniej ochrony danych, jest Ogólne Rozporządzenie o Ochronie Danych (RODO)[122], które weszło w życie w maju 2018 roku. Cel rozporządzenia ustanawiającego wspólny zbiór zasad ochrony danych osobowych dla wszystkich przedsiębiorstw działających w UE jest dwojaki: po pierwsze zapewnia ono bezpieczeństwo danych osobowych obywateli – fundamentalne prawo w UE – a zarazem gwarantuje swobodny przepływ danych między państwami członkowskimi – rzecz niezbędna firmom, aby operować na zglobalizowanym rynku. Prawny kształt RODO odbiega od NIS, gdyż jest to rozporządzenie, ma zatem bezpośrednie zastosowanie w państwach członkowskich. Trzy z 28 krajów UE nie osiągnęły jednak nadal (stan na 24 lipca 2019) zgodności swoich przepisów dotyczących ochrony danych z zasadami unijnymi[123]. Mimo rozpoczęcia wdrażającego RODO procesu legislacyjnego w parlamencie w kwietniu 2017 roku Słowenia należy do państw, które do tej pory nie wprowadziły rozporządzenia[124].

RODO wzmocniło rolę krajowych organów ochrony danych (OOD, ang. DPAs), wyposażając je w nowe uprawnienia w związku z egzekwowaniem europejskich przepisów. Są one na przykład odpowiedzialne za wydawanie wytycznych na temat kluczowych aspektów RODO w celu wspierania implementacji rozporządzenia na poziomie krajowym, mają prawo nakładać „skuteczne, proporcjonalne i odstraszające”[125] grzywny do wysokości 4% całkowitych rocznych przychodów lub 20 milionów euro – zależnie od tego, która wartość jest wyższa – na organizacje naruszające wymogi przepisów. Dodatkowo OOD włączono w nowe ogólnoeuropejskie mechanizmy współpracy oraz Europejską Radę Ochrony Danych, co pozwala im lepiej koordynować działania. Według najnowszego raportu wspomnianej rady, przedstawionego Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych Parlamentu Europejskiego w lutym 2019 roku[126], zarejestrowano łącznie 206326 spraw[127], w tym 94622 skargi konsumenckie, 64684 powiadomienia o naruszeniu ochrony danych zgłoszone przez ich administratorów oraz 47020 innych przypadków. Choć brakuje rozbicia statystyk na poszczególne kraje, można pokusić się o stwierdzenie, że wykorzystanie tych uprawnień w EŚW pozostaje na niewysokim poziomie w porównaniu z innymi regionami UE. *De facto* urzędy nadzoru

122 Parlament Europejski i Rada (UE), *Rozporządzenie 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)*, Dz. U. UE L 119, s. 1–88, 4 maja 2016.

123 Komisja Europejska, *Ogólne rozporządzenie o ochronie danych przynosi efekty, ale konieczne są dalsze działania*, 24 lipca 2019, [online]: https://ec.europa.eu/commission/presscorner/detail/pl/IP_19_4449.

124 Ibidem.

125 Motyw 151 RODO.

126 Europejska Rada Ochrony Danych, *First overview on the implementation of the GDPR and the roles and means of the national supervisory authorities*, 2019, s. 7 i 12, [online]: https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/LIBE/DV/2019/02-25/9_EDPB_report_EN.pdf

127 Liczba obejmuje przypadki zarejestrowane przez organy nadzoru z 31 krajów EOG.

nałożyły kary w zaledwie 11 krajach – o łącznej wartości około 56 milionów euro, w tym rekordowe 50 mln we Francji. Trzy państwa EŚW – Czechy, Słowacja i Słowenia – należą do krajów, w których wciąż nie nałożono żadnych grzywien w związku z RODO.

Ponieważ każde z państw dysponuje własną wizją wdrażania RODO, trudno określić, które z nich są najbardziej zaawansowane czy zaangażowane wyłącznie na podstawie liczby bądź wysokości kar. Kilka przykładów z regionu Trójmorza zilustruje różnorodność podejść do kwestii wprowadzania tego rozporządzenia w życie oraz systemu kar.

Austria ustanowiła system, wedle którego za wykryte naruszenia RODO sprawca otrzymuje najpierw od austriackiego OOD ostrzeżenie, a kara nakładana jest dopiero przy braku poprawy albo ujawnieniu kolejnego naruszenia. Jak dotąd tamtejszy regulator zastosował grzywnę tylko pięć razy, w każdym przypadku w związku z nielegalnym nagrywaniem obrazu[128].

Podobną ścieżką pod względem liczby grzywien kroczy Łotwa, jeden z krajów, w których nałożono w pierwszym roku obowiązywania RODO nieliczne kary. Właściwie litewski organ ochrony danych z zasady stara się, zamiast karać, służyć organizacjom radą i pomocą co do przestrzegania wymogów RODO. Takie podejście stosują również inne kraje Trójmorza, na przykład Bułgaria i Chorwacja[129].

Litwa wykazuje natomiast większą aktywność i na początku 2019 roku ogłosiła nazwy 75 organizacji, które czeka w ciągu roku inspekcja w sprawie stosowania się do RODO. Po ukończeniu postępowań miejscowy OOD przedstawi zbiór ogólnych wskazówek dotyczących najczęstszych problemów z przestrzeganiem zasad[130].

Powyższe trzy przykłady pokazują, że nastawienie w regionie z reguły polega na tym, by zapobiegać, nie karać. Tendencja rzadszego uciekania się do kar za naruszenia RODO zdaje się jednak zanikać. W ostatnich miesiącach mnożą się doniesienia o przypadkach nakładania grzywien. Przykładem sprawy na dużą skalę jest ogromny wyciek danych w lipcu 2019 roku w Bułgarii, w ramach którego skradziono informacje na temat 5 milionów tamtejszych obywateli, co spotka się z karą w wysokości 2,6 mln euro[131].

BUDOWA ZDOLNOŚCI CYBERBEZPIECZEŃSTWA W REGIONIE – AKT O CYBERBEZPIECZEŃSTWIE I DALSZE DZIAŁANIA

Trzeci wreszcie i najnowszy zbiór przepisów przyjęty na poziomie unijnym to akt o cyberbezpieczeństwie[132], obowiązujący od czerwca 2019 roku. Stojąca za nim koncepcja to tworzenie spójniejszej sytuacji w dziedzinie cyberbezpieczeństwa na obszarze UE, zwłaszcza przez wprowadzenie ogólnounijnych reguł certyfikacji produktów, usług i procesów teleinformatycznych. Spójność wzrośnie więc automatycznie także w regionie EŚW.

W znacznej większości krajów powstają również niezależne od prawa Unii narodowe zalecenia i strategie rozwoju cyfrowego. Mogą, nie będąc częścią prawodawstwa, odzwierciedlać państwowy bądź regionalny stosunek do cyberbezpieczeństwa. Dokumenty takie stworzono w każdym z 12 krajów, na których się skupiamy[133]. Już ten fakt podkreśla,

128 „Der Standard", *Fünf Strafen in Österreich seit Einführung der DSGVO*, 12 marca 2019, [online]: https://www.derstandard.at/story/2000099395386/fuenf-strafen-in-oesterreich-seit-einfuehrung-der-dsgvo.

129 Neil Hodge, *GDPR enforcement varies widely by country*, „Compliance Week", 19 lipca 2019, [online]: https://www.complianceweek.com/gdpr/gdpr-enforcement-varies-widely-by-country/27436.article.

130 Ibidem.

131 IAAP, *Bulgarian DPA issued BGN 5.1M fine to revenue agency for GDPR violations*, 2019, [online]: https://iapp.org/news/a/bulgarian-dpa-issued-bgn-5-1m-fine-to-national-revenue-agency-for-gdpr-violations/.

132 Parlament Europejski i Rada (UE), *Rozporządzenie 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie)*, Dz. U. UE L151/15, 7 czerwca 2019.

133 ENISA, *National Cyber Security Strategies (NCSSs) Map*, [online]: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map.

że świadomość cyberzagrożeń i potrzeby bezpieczeństwa wydatnie wzrosła i jest uwzględniana, a warto także zauważyć, że niektóre kraje EŚW należą do najambitniejszych i najaktywniejszych pod względem ochrony przed cyberzagrożeniami. Polska znajduje się w tym gronie. Po przyjęciu Krajowych Ram Polityki Cyberbezpieczeństwa na lata 2017–2022 Ministerstwo Cyfryzacji sformułowało niedawno nowy projekt ich zastąpienia na okres 2019–2024 dla dostosowania do nowych zagrożeń. Co ważne, proponowana strategia wprowadza odniesienie do partnerstwa publiczno-prywatnego, o którym krajowe ramy nie wspominały, ma też na celu rozwój krajowego systemu cyberbezpieczeństwa powstałego w 2018 oraz działania sprzyjające współpracy na arenie międzynarodowej[134]. W podobnym duchu wyznaczyła strategię cyberbezpieczeństwa Litwa, nadając jej charakter pod pewnymi względami unikatowy i stając się jednym z najlepiej przygotowanych na cyberataki krajów na świecie według Global Security Index Międzynarodowego Związku Telekomunikacyjnego[135]. Do zalet litewskiego planu należy przekazanie, w imię optymalizacji sprawności organizacyjnej, całej odpowiedzialności za politykę cyberbezpieczeństwa ministerstwu obrony. Unika się tym samym rozdrobnienia, nierzadko prowadzącego do zwiększonej podatności na zagrożenia i niepewności przy kreśleniu ich całościowego obrazu. Ponadto litewski rząd rozwija bezpieczną sieć, odrębną od publicznych sieci komunikacji, która nie przestanie działać w razie kryzysu lub wojny oraz pozwoli władzom szybciej i skuteczniej reagować na incydenty w cyberprzestrzeni[136].

CYBERPRZESTĘPCZOŚĆ

Pierwszy wiążący traktat międzynarodowy o przestępstwach popełnionych w sieci, budapeszteńską Konwencję Rady Europy o cyberprzestępczości, ratyfikowało wszystkich 28 członków UE, wliczając każde z państw Trójmorza[137]. Konwencja opierała się na idei uniemożliwienia powstania „bezpiecznych przystani" korzystających ze zróżnicowania ram prawnych w poszczególnych krajach oraz zapewnienia zharmonizowanego podejścia do walki z tym typem przestępstw. Współczesna cyberprzestępczość nie zna fizycznych granic, toteż umowa ta zachęca do współpracy i wzajemnego wsparcia pomiędzy sygnatariuszami, natomiast obecnie opracowuje się dodatkowy drugi protokół odnoszący się do usunięcia barier na drodze do elektronicznego dostępu organów sądowych i policji do dowodów elektronicznych. W EŚW tempo ratyfikowania konwencji bywało rozmaite – Chorwacja na przykład przyjęła ją jako jedno z pierwszych państw, podczas gdy Polska czekała do roku 2015. Trzeba jednak zauważyć, że RP zmodernizowała prawodawstwo i wprowadziła do Kodeksu karnego poprawki dotyczące licznych rodzajów cyberprzestępstw już w 2004[138]. Raport European Cybercrime Centre (EC3)[139], komórki Europolu, podkreśla nadal wysokie wskaźniki takich przestępstw w regionie EŚW, przykładem czołowe miejsca Austrii i Węgier w klasyfikacji e-maili ze szkodliwym oprogramowaniem i phishingiem. W raporcie podkreślono, że organy ścigania przyglądają się szerokiemu spektrum cyberataków, ale oszustwa płatnicze to raczej problem narastający, a w szczególności Rumunię i Bułgarię nadal uważa się za grające w tej kwestii niechlubną rolę.

134 Ministerstwo Cyfryzacji, *Rozpoczynamy konsultacje projektu Strategii Cyberbezpieczeństwa*, 5 sierpnia 2019, [online]: https://www.gov.pl/web/cyfryzacja/rozpoczynamy-konsultacje-projektu-strategii-cyberbezpieczenstwa.

135 ITU, *2018 Global Cybersecurity Index (v3)*, 2018, [online]: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.

136 Ministerstwo Obrony Narodowej Republiki Łotewskiej, *Cyber Security Council discussed EU and Lithuanian cyber security initiatives*, 19 lutego 2019, [online]: http://kam.lt/en/news_1098/current_issues/cyber_security_council_discussed_eu_and_lithuanian_cyber_security_initiatives.html.

137 Rada Europy, *Chart of signatures and ratifications of Treaty 185. Status as of 06/09/2019*, [online]: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=HCKz9uSV.

138 Leslie Holmes, *Cybercrime in Russia and Central and Eastern Europe*, rozdział *Official Responses to Cybercrime*, [w:] *Digital Eastern Europe*, red. William Schreiber i Marcin Kosienkowski, Wrocław 2015.

139 European Cybercrime Centre, *Internet Organised Crime Threat Assessment. IOCTA 2018*, [online]: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment.

PODSUMOWANIE

Obecna sytuacja legislacyjna w zakresie cyberbezpieczeństwa w rejonie Trójmorza jest niejednolita. Niektóre kraje, na przykład nadbałtyckie i Polska, wykazują wysoki poziom ambicji oraz świadomości problemu, inne zaś przejmują się zagrożeniami raczej w mniejszym stopniu lub wprost z trudem stawiają czoła wyzwaniu, potrzebując zatem silniejszego wsparcia. Niemniej warto dostrzec dwie rysujące się tendencje. Po pierwsze – jak wskazuje badanie transpozycji dyrektywy NIS w krajach EŚW – region skłania się ku poszerzaniu grona sektorów chronionych przed cyberzagrożeniami. Wskazuje to na pewien szczebel uświadomienia i gotowości do działania w tej dziedzinie. Po drugie – przede wszystkim dzięki staraniom Unii Europejskiej i w związku z niedawnym wejściem w życie aktu o cyberbezpieczeństwie – harmonizacja odpowiednich regulacji prawnych w obrębie Unii będzie postępować, co niewątpliwie stanowi dla przedsiębiorstw pomyślną wieść.

REGION TRÓJMORZA W KONTEKŚCIE EKOLOGICZNYM I ŚRODOWISKOWYM

WPŁYW NA ŚRODOWISKO

Ochrona środowiska stała się w kilku ostatnich latach kwestią doniosłą, a jej istotność zapewne nie zmaleje w nadchodzącej dekadzie. Obawy związane z niedoborem surowców, zanieczyszczeniem powietrza, wody i gleby, śladem węglowym czy produkcją towarów opartą na zrównoważonym rozwoju widnieją wysoko na liście dylematów konsumenckich, ale też producenckich. Wobec szybkiego wzrostu branży teleinformatycznej (ICT) na świecie pojawiają się nowe elementy zagadnienia. Ocenia się, że pojedynczy e-mail może odpowiadać za emisję do atmosfery 4 g CO_2 – 50 g, jeśli zawiera długi załącznik[140]. Sytuacja branży ICT i cyberbezpieczeństwa jest zatem dwuznaczna: z jednej strony rozwój technologii stanowi wyjątkową okazję do redukcji emisji dwutlenku węgla i pójścia w kierunku zielonej gospodarki krajowej, z drugiej jednak rodzi nowe pytania o zużycie energii, a szerzej ślad węglowy produkcji oraz wykorzystania technologii informatycznych i komunikacyjnych. Ten rozdział poświęcony będzie analizie wpływu takich technologii na środowisko w regionie Trójmorza.

Kwestie związane z ich wykorzystaniem są liczne i dotyczą całego cyklu życia produktów. Przede wszystkim wytwarzanie urządzeń cyfrowych wymaga znacznej energii i wielu zasobów, tworząc rozmaite problemy powiązane z niedoborem zasobów – na przykład metali ziem rzadkich – bądź zanieczyszczeniem takiego czy innego typu spowodowanym przez samą produkcję albo przez eksploatację zasobów. Po drugie urządzenia oraz infrastruktura, na których opiera się działanie ICT, zużywają

140 Mike Berners-Lee, *How Bad are Bananas? The Carbon Footprint of Everything*, London: Profile Books, 2010, s. 15.

Stanowi wyjątkową szansę ograniczenia emisji CO_2, wspierając zwrot wielu sektorów gospodarki w stronę zielonych technologii.

Rodzi pytania o zużycie energii i ślad węglowy przy tworzeniu i wykorzystaniu technologii teleinformatycznych.

niemałą ilość energii, przyczyniając się tym samym do zwiększania światowego poziomu emisji gazów cieplarnianych, jeśli prąd ten nie pochodzi z czystych źródeł. Wreszcie recykling i utylizacja zużytych produktów ICT jest istotnym zagadnieniem, na które nie znaleziono jeszcze zadowalającej odpowiedzi.

MOTOR CYFROWYCH PRZEMIAN

Ogólny stan produkcji i zużycia energii w Europie Środkowej i Wschodniej zwykle przedstawia się jako marny pod względem ekologicznym. Dzieje się tak głównie z powodu dwóch państw, Polski i Czech, oraz ich historii wydobycia i spalania węgla. W roku 2018 Polska była miejscem wydobycia aż 86% węgla kamiennego w UE – używanego zwłaszcza do ogrzewania pomieszczeń mieszkalnych i handlowych – zostawiając daleko z tyłu drugiego głównego producenta, Czechy, odpowiedzialne za 4,5%[141]. Liczby te zmalały względem poziomu z roku 2012. Trzeba jednak zauważyć, że w tych dwu państwach EŚW spadek był mniej znaczący niż w trzech innych krajach wydobywających węgiel (Polska: –20%, Czechy: –39%, zaś Niemcy: –76%, Wielka Brytania: –84%, Hiszpania: –86%). W kwestii zużycia węgla kamiennego Polska ponownie znajduje się na czołowym miejscu – 32% całości spalania w UE. Jeśli chodzi o węgiel brunatny – używany niemal wyłącznie jako paliwo do produkcji energii elektrycznej – Polska zużyła w 2017 16% ogólnej liczby dla UE, na kolejnych pozycjach znalazły się Czechy (10%), Bułgaria (9%) i Rumunia (7%). Zarówno wydobycie, jak i zużycie tych paliw ma wyraźnie negatywny wpływ na środowisko, szczególnie z powodu wzrostu zanieczyszczenia powietrza. Warto wziąć powyższe statystyki pod uwagę, ponieważ węgiel kamienny i brunatny służy do produkcji energii, która napędza urządzenia, centra danych i sieci ICT, podobnie jak cały przemysł produkcyjny na nich oparty.

Ogółem w EU28 zużycie energii w branży teleinformatycznej (wyłączając produkcję) wyniosło w 2011 roku 214 terawatogodzin (TWh), co stanowi 7,7% łącznego zużycia energii. Odsetek ten, głoszą szacunki, wzrośnie w 2020 do 8,1% i sięgnie 259 TWh[142]. Zużycie prądu w domach i biurach stanowiło 66% łącznego zużycia energii w tym sektorze i ocenia się, że zmaleje ono do 2020 o jeden procent. Zarazem zużycie przez centra danych i sieci telekomunikacyjne wzrośnie o 35 i 150%, przede wszystkim z racji intensywnego wykorzystania mobilnych usług internetowych oraz sprawniejszych i dających większe możliwości sieci komórkowych. Oznacza to, że zgodnie z przewidywaniami w roku 2020 udział centrów danych i sieci telekomunikacyjnych w ogólnounijnym zużyciu energii elektrycznej sięgnie 3,8% w porównaniu z 2,6% w 2011. W przypadku samego regionu EŚW szacuje się średnią roczną stopę wzrostu rynku centrów danych na 5% w okresie 2018–2024[143]. Łatwo zatem zrozumieć, że skutki rozrostu tego sektora są potencjalnie groźne dla środowiska, jeśli nie będzie on zasilany bezemisyjnymi źródłami energii.

Pewne aspekty zużycia energii przez przemysł na obszarze EŚW nastrajają jednak bardziej optymistycznie. O ile końcowe jej zużycie w przemyśle UE-28 zmalało między 2006 a 2017 o 12,8%[144], konsumpcja energii odnawialnej i biopaliw wzrosła o 28,4%, stanowiąc oznakę ogólnego polepszenia źródeł energii przemysłu UE[145]. W odniesieniu do udziału energii ze źródeł odnawialnych i biopaliw

141 Eurostat, *Coal production and consumption statistics*, 2019, [online]: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Coal_production_and_consumption_statistics#Consumption_and_production_of_hard_coal.

142 Dyrekcja Generalna ds. Społeczeństwa Informacyjnego i Mediów (Komisja Europejska), Politechnika Berlińska, Öko-Institut e.V, *Study on the practical application of the new framework methodology for measuring the environmental impact of ICT – cost/benefit analysis*, 2014, [online]: https://publications.europa.eu/en/publication-detail/-/publication/d2235b7a-2c60-4937-a87d-e46e23f44f21/language-en/format-PDF/source-search#.

143 Research and Markets, *Central and Eastern Europe Data Center Market – Investment Analysis and Growth Opportunities 2019–2024*, 2019.

144 Eurostat, *Final energy consumption in industry by type of fuel*, [online]: https://ec.europa.eu/eurostat/databrowser/view/ten00129/default/table?lang=en.

145 Ibidem.

Całkowite zużycie energii w przemyśle w UE-28

2006

zmniejszyło się o **12,8%**

2017

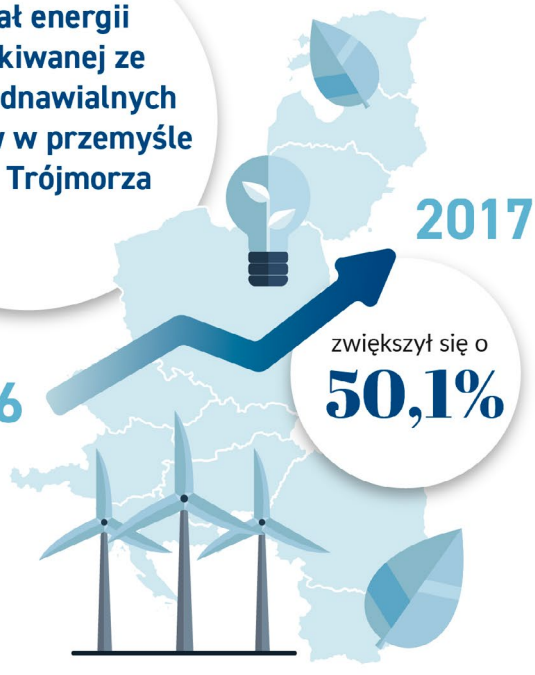
Zużycie w przemyśle energii pozyskiwanej z biopaliw i źródeł odnawialnych

2006

zwiększyło się do **28,4%**

2017

Udział energii pozyskiwanej ze źródeł odnawialnych i biopaliw w przemyśle krajów Trójmorza



2006

zwiększył się o **50,1%**

2017

w przemyśle EŚW wzrost ten był jeszcze wyraźniejszy i osiągnął 50,1% w latach 2006–2017. Problem wpływu przemysłu na środowisko znalazł w krajach regionu oddźwięk, a przedsiębiorstwa podjęły pewne wysiłki na rzecz poprawy sytuacji. Ograniczenie rozwoju sektora ICT jest niemożliwe i byłoby szkodliwe, ale zmiana źródeł energii zasilającej tę branżę to krok we właściwym kierunku.

Ponadto zaczynają się pojawiać inicjatywy zmierzające do ograniczenia między innymi wpływu wciąż rosnącego zużycia energii przez centra danych na środowisko i bezpieczeństwo dostaw prądu. Na poziomie unijnym sformułowano na przykład Kodeks Postępowania w Centrach Danych na rzecz Efektywności Energetycznej[146] wraz z grupą w ramach platformy E3P (European Energy Efficiency Platform). Większość uczestników pochodzi z Europy Zachodniej, ale niedawne zapisanie się przez Polskę to sygnał zmian na lepsze ze strony EŚW[147].

ZIELONA CYBERPRZESTRZEŃ

Przechodząc od rozważań o zużyciu energii przez urządzenia i infrastrukturę ICT do okazji stwarzanych przez te narzędzia i wiążących się z nimi metod poprawy sytuacji, możemy wskazać na pewne optymistyczne skutki, które z dużym prawdopodobieństwem zajdą. Inteligentne urządzenia i aplikacje, szczególnie w sektorze energetycznym, mogą mieć duży wpływ, pomagając ograniczyć szkody wyrządzane środowisku przez produkcję i konsumpcję energii.

Unia w pakiecie Czysta energia dla wszystkich Europejczyków wyznaczyła sobie następujące cele na rok 2030:

- zmniejszenie emisji gazów cieplarnianych o 40% (w porównaniu z poziomem z 1990 roku);
- wzrost efektywności energetycznej o co najmniej 32,5%;
- wzrost udziału energii odnawialnej do 32%.

Rozwiązania teleinformatyczne mogą wesprzeć osiągnięcie każdego z tych zamierzeń.

Rola techniki w ograniczaniu emisji gazów cieplarnianych jest znacząca. W połączeniu z już wdrażanymi rozwiązaniami inżynierskimi, przykładem sekwestracja CO_2, ICT – umożliwiając dostęp do danych w czasie rzeczywistym i usprawnioną automatyzację w różnorodnych branżach przemysłu – dysponuje realnym potencjałem opanowania problemów z węglem. Po analizie dwunastu zastosowań ICT w raporcie BT Group znalazł się wniosek, że w UE do 2030 możliwa jest wyraźna redukcja emisji dwutlenku węgla, wynosząca 1,5 Gt. Według raportu jej wartość wyniosłaby prawie 19 razy więcej niż prognozowany ślad węglowy unijnego sektora ICT w tym samym roku, a zarazem 37% łącznych unijnych emisji gazów cieplarnianych z 2012[148]. Równocześnie poprawa efektywności energetycznej za sprawą ICT może też tworzyć wartość biznesową. Rozwój tego sektora przyniesie wedle szacunków 678 mld euro dodatkowych przychodów i do 643 mld euro oszczędności. Raport stwierdza wreszcie, że wywołany zastosowaniem ICT wzrost efektywności energetycznej może stać się źródłem zmniejszenia emisji węglowych o 0,8 Gt, czyli 53% łącznego spadku w UE.

W zakresie drugiego z celów potencjał technologii ICT również jest spory. Już w roku 2008 Komisja Europejska ogłosiła, że będzie promować wykorzystanie informatyki, aby poprawiać efektywność energetyczną w całej gospodarce. W szczególności czujniki gazu zawierające i sprzęt, i oprogramowanie mogą wyraźnie wpłynąć na zużycie energii i zmniejszyć emisje gazów cieplarnianych w sektorze

146 Komisja Europejska, *2019 Best Practice Guidelines for the EU Code of Conduct on Data Centre Energy Efficiency*, [online]: https://ec.europa.eu/jrc/en/energy-efficiency/code-conduct/datacentres.

147 EU Joint Research Centre, European Energy Efficiency Platform (E3P), [online]: https://e3p.jrc.ec.europa.eu/communities/data-centres-code-conduct.

148 BT, *The role of ICT in reducing carbon emissions in the EU*, 2016, [online]: https://www.btplc.com/Purposefulbusiness/Ourapproach/Ourpolicies/ICT_Carbon_Reduction_EU.pdf.

przemysłowym i transportowym. Sprawność procesów w przemyśle obejmuje bowiem uważne monitorowanie stężeń gazów i przepływu powietrza podczas spalania. Czujniki, zbierając dane w trudnych warunkach – takich jak instalacje spalania, pojazdy lądowe i morskie – i przekazując je na bieżąco, są w stanie przyczynić się do potrzebnych modyfikacji. Inne zastosowanie zwiększające efektywność energetyczną w budynkach to rozpowszechnienie inteligentnych liczników i inteligentnych sieci przesyłowych, zdolnych zmniejszyć roczne zużycie energii gospodarstwa domowego nawet o 9%[149]. Celem Unii jest zastąpienie do roku 2020 co najmniej 80% liczników prądu urządzeniami inteligentnymi. Ponieważ systemy te pozwalają konsumentom śledzić swoje zużycie energii w czasie rzeczywistym, umożliwiają także dostosowanie go w cyklu dobowym w zależności od na przykład ceny. W połączeniu z urządzeniami Internetu Rzeczy inteligentne systemy energetyczne potrafią szacować zapotrzebowanie w budynku i dopasować zużycie. Konsekwentnie uwzględniać trzeba wyzwania w dziedzinie cyberbezpieczeństwa wynikające z wdrażania takich liczników. Digitalizacja naraża właściwie całe połacie energetyki na nowe typy ryzyka, które można zwalczać tylko za pomocą stosowania zasady cyberbezpieczeństwa już od etapu projektu. Sektor energii objęto różnymi ramami prawnymi dotyczącymi cyberbezpieczeństwa, jednak jego nietypowość sprawia, że potrzeba tu legislacji osobnej. W tym celu Komisja Europejska z początkiem kwietnia 2019 roku przyjęła zalecenia na temat cyberbezpieczeństwa w energetyce[150].

Przewodnik po dobrych praktykach efektywności energetycznej dla Europy Środkowej i Południowo-Wschodniej Komisji Europejskiej zwraca uwagę na kilka ponadnarodowych projektów podejmowanych obecnie dla poprawy tej efektywności w przemyśle i biznesie oraz ogrzewaniu, klimatyzacji i ciepłownictwie. Wśród nich warto wymienić na przykład mogący mieć znaczenie dla regionu projekt PeakApp. Składa się on z aplikacji na smartfony i komputery, wprowadzając element gry w zachęcaniu do oszczędzania energii i korzystania z jej czystych i tanich źródeł[151].

ICT może również przydać się istotnie w zwiększaniu udziału energii odnawialnej. Inteligentne liczniki pozwalają właściwie konsumentom na produkcję energii i dostarczanie jej do sieci, zwłaszcza w przypadku źródeł odnawialnych. Informacja w czasie rzeczywistym o zużyciu i produkcji energii umożliwia gospodarstwom domowym stanie się jej dostawcami, tworząc w ten sposób inteligentną sieć dwukierunkową. Praktyka sprzyjania podłączaniu źródeł odnawialnych do ogólnej sieci mogłaby stanowić w krajach EŚW drogę przemiany i odejścia od generowania energii opartego na węglu. To efektywne narzędzie przeskoku w stronę gospodarki bardziej przyjaznej środowisku.

Można odnieść wrażenie, że w zakresie zużycia energii oraz emisji gazów cieplarnianych ICT pomoże zbliżać się do ogólnounijnych celów korzystania z czystej energii wedle koncepcji na rok 2050. W innych sferach, takich jak monitorowanie zanieczyszczenia gleby czy wody, gospodarowanie lasami czy szacowanie klęsk żywiołowych i odpowiedź na nie, narzędzia cyfrowe również okazują się bardzo użyteczne. Przyczyniając się do innowacyjności i wydajności energetyki, jej rosnące ucyfrowienie zarazem wystawia tę infrastrukturę na nowe niebezpieczeństwa, na przykład cyberataki, stanowiące zagrożenie bezpieczeństwa dostaw energii i prywatności danych konsumenckich. Z uwagi na sytuację geopolityczną region EŚW mierzy się ze zwiększoną podatnością

149 Komisja Europejska, *Smart grids and meters*, [online]: https://ec.europa.eu/energy/en/topics/markets-and-consumers/smart-grids-and-meters/overview.

150 Komisja Europejska, *Commission Recommendation of 3.4.2019 on cybersecurity in the energy sector*, 3 kwietnia 2019, [online]: https://ec.europa.eu/energy/sites/ener/files/commission_recommendation_on_cybersecurity_in_the_energy_sector_c2019_2400_final.pdf.

151 Komisja Europejska, *Guide on good practice in energy efficiency for Central and South Eastern Europe*, 2018, s. 24, [online]: https://s3platform.jrc.ec.europa.eu/documents/20182/238542/Guide+on+good+practice+in+energy+efficiency+for+Central+and+South+Eastern+Europe/3f8a1d96-e259-4ab7-8da0-723e389f4abf.

tego sektora. Ataki na sieć ukraińską w 2015 roku wywołały w środku zimy przerwy w dostawie prądu, które dotknęły 225 000 osób[152], co stanowi adekwatny przykład, jak masowe i szkodliwe mogą być skutki takich działań. Przejście w kierunku sieci ucyfrowionej i połączonej to bez wątpienia nieodzowny krok, który powinno się podjąć wraz z przyjęciem zasady cyberbezpieczeństwa już na etapie projektowania.

PODSUMOWANIE

Reasumując, postęp technologii informacyjnych i komunikacyjnych to miecz obosieczny, będący w stanie przyczynić się i do ochrony, i niszczenia środowiska, jeśli nie spożytkuje się go zgodnie z zasadami zrównoważonego rozwoju. W tym kontekście region Europy Środkowej i Wschodniej – z racji obejmującej spory udział paliw kopalnych produkcji i zużycia energii oraz oczekiwanego szybkiego wzrostu lokalnego sektora informatyczno-komunikacyjnego – powinien dokładać starań i podejmować kroki, aby zmierzać w stronę zielonej energetyki. Omawiane technologie stanowią cenne narzędzia na tej drodze. Jednak z uwagi na nowe zagrożenia przez nie wprowadzane podstawowe znaczenie zyskuje równoległe rozwijanie w energetyce kultury cyberbezpieczeństwa. Firmy Trójmorza, jako szeroko narażone na cyberzagrożenia, najlepiej też nadają się, by dostarczać narzędzia i rozwiązania w obliczu nowych wyzwań. Wprowadzanie technologii informatycznych to zatem dla regionu podwójna szansa, by rozwinąć gospodarkę na bazie pozytywnej transformacji sektora energii.

152 Cybersecurity and Infrastructure Security Agency, *ICS Alert (IR-ALERT-H-16-056-01) Cyber-Attack Against Ukrainian Critical Infrastructure*, [online]: https://www.us-cert.gov/ics/alerts/IR-ALERT-H-16-056-01.

ANALIZA PESTLE

POLITYKA	GOSPODARKA	SPOŁECZEŃSTWO
• **Wrażliwy politycznie obszar**, stanowiący zewnętrzną granicę zarówno UE, jak i NATO (tzw. wschodnią flankę), determinuje silną korelację między sytuacją geopolityczną a cyberzagrożeniami. • **Rosja** traktuje region jako szczególną sferę własnych wpływów. Można zaobserwować rosnące zainteresowanie **ChRL** w ramach dedykowanego formatu 16+1. Brexit oraz ryzyko konfliktu na Morzu Południowochińskim wpłynie na spadek zainteresowania regionem **Wielkiej Brytanii i Stanów Zjednoczonych.** • Przechodzący głębokie zmiany strukturalne region Europy Środkowo-Wschodniej rozwija różnorodne **wspólne inicjatywy regionalne**, m.in. Trójmorze oraz V4+. Ze względu na odmienne cele i uwarunkowania polityczne wyzwaniem pozostaje zapewnienie spójności realizowanych przedsięwzięć. • Wielowymiarowe działania ofensywne prowadzone w cyberprzestrzeni stały się w regionie Trójmorza ważnym elementem prowadzonych **działań hybrydowych**, zwłaszcza w zakresie dezinformacji, szpiegostwa przemysłowego i ataków na infrastrukturę krytyczną. • Należy się spodziewać, że wraz z planowanym wzrostem ilościowym i jakościowym wojsk stacjonujących przy granicach zewnętrznych UE i NATO wielowymiarowe ofensywne **cyberoperacje będą się nasilać**.	• Dwanaście państw członkowskich Trójmorza obejmuje trzy dawne republiki sowieckie, sześć byłych państw przynależących do Paktu Warszawskiego i dwa należące do byłej Jugosławii. • Ogólny średni **wzrost PKB** w regionie w latach 2017–2030 prognozowany jest na ok. 2,4% w skali roku (MFW). Nieco niższą wartość przedstawia OECD, prognozując średni wzrost w granicach 2%. • **Prognozy demograficzne** nie są dla regionu pozytywne. Właściwie wszystkie państwa, z wyjątkiem AT, odnotują znaczny spadek populacji oraz starzenie społeczeństwa. • Zgodnie ze wskaźnikiem DESI 2019 większość krajów obszaru Trójmorza – poza EE i AT – notuje **innowacyjność** niższą niż średnia dla UE-28. RO wespół z BG plasują się na ostatnich miejscach w obrębie UE-28. • W latach 2006–2016 **wydatki B+R** w regionie Trójmorza wzrosły całościowo o 79,2%, podczas gdy dla UE ten odsetek wyniósł ponad połowę mniej, tj. 36,2%. Największy wzrost odnotowano w BG (230,2%), SK (193,1%) i PL (173,5%). • We wszystkich krajach regionu Trójmorza rośnie **zatrudnienie w sektorze ICT** względem ogółu zatrudnionych, przy czym odsetek ten jest najwyższy w EE (3,69%), LV (3,59%) i HU (3,51%). Najniższy udział zatrudnienia w sektorze technologii odnotowano w RO (2,27%), PL (2,29%) i HR (2,34%).	• Kraje Trójmorza są zróżnicowane pod względem społecznego potencjału cyfryzacji. EE przewyższa (13,3%), a RO zbliża się (10,6%) **odsetkiem absolwentów kierunków teleinformatycznych** do średniej dla UE-28 (11%). BG, LT i PL znajdują się na przeciwległym biegunie zestawienia. • Sześć państw (AT, RO, LT, PL i CZ) dysponuje proporcjonalnie większym **odsetkiem absolwentów kierunków ścisłych** takich jak inżynieria, produkcja i budownictwo niż średnia unijna. • W państwach Trójmorza, podobnie jak w UE, więcej mężczyzn niż kobiet posiada co najmniej **podstawowe umiejętności cyfrowe**. Rośnie odsetek absolwentów kierunków STEM. W PL i RO ok. 40% absolwentów kierunków technicznych stanowiły kobiety. • Wśród użytkowników Internetu w AT (41,2%), LT (41,1%) SK (40,5%), EE (39,5%) oraz SI (37,6%) posiadanie podstawowych umiejętności cyfrowych jest bardziej powszechne niż w UE-28 (37,3%). • Region dysponuje bardzo uzdolnionym zapleczem **programistów**. PL znajduje się (wraz z RU i za ChRL) na drugim miejscu rankingu zdobywców medali Międzynarodowej Olimpiady Informatycznej (IOO) do 2019 r. W pierwszej dziesiątce uplasowały się również trzy inne państwa regionu inicjatywy: RO, BG oraz SK. • Kraje UE zmagają się z **niedoborem pracowników IT** – 53% pracodawców w 2018 r. miało problem z ich zatrudnieniem. W regionie trudność ta jest najbardziej powszechna w dwóch państwach – CZ (79%) i AT (78%).

TECHNOLOGIE	PRAWO	ŚRODOWISKO
• Kraje Trójmorza charakteryzują się **bardzo wysoką prędkością łącz internetowych**. LT, EE i LV znajdują się na liście 23 krajów z najwyższą prędkością na świecie – odpowiednio 27,42, 27,91 i 28,63 Mb/s), co może stanowić o ich przewadze konkurencyjnej. • Dynamicznie rozwija się sektor **AI**. W samej tylko PL istnieje aż 110 startupów zajmujących się AI, w EE – 46, na LV – 26, na LT – 29, a w RO – 32. Istotne znaczenie mają inwestycje i wsparcie rządowe wynikające z narodowych strategii AI. Mimo wyznaczenia przez KE terminu opracowania strategii AI, do połowy 2019 roku aż pięć krajów Trójmorza (AT, HR, PL, SI oraz HU) nie zdążyło jej opublikować. • Kraje Trójmorza są aktywne w sferze rozwoju **blockchain**, co obrazuje liczba powstających startupów, dedykowanych wydarzeń, jak i planowanych przez sektor prywatny inwestycji. Rośnie zainteresowanie informatyką kwantową, z uwagi jednak na względną niedojrzałość technologii jej masowe zastosowanie jest ograniczone. • W 2019 region zainwestował ponad 11,2 mld USD w **Internet Rzeczy** (IoT), co stanowi ok. 19,5% wzrost względem 2018. Rośnie świadomość znaczenia oraz popyt na rozwiązania IoT, szczególnie na HU i w CZ. • Dynamika wdrażania sieci **5G** w krajach regionu jest różnorodna – od liderów w postaci AT i państw bałtyckich przez coraz aktywniejsze RO, PL i HU.	• **Dyrektywa na rzecz bezpieczeństwa sieci i systemów informatycznych (NIS)** była pierwszą regulacją przyjętą na terenie całego Trójmorza zgodnie z celami ustalonymi w unijnej strategii cyberbezpieczeństwa z roku 2013. To także pierwszy ogólnounijny zbiór przepisów w tej dziedzinie. • Poza RO, BG i HU wszystkie państwa 3S przy transpozycji dyrektywy NIS skorzystały z okazji **dodania kolejnych branż definiowanych jako operatorzy usług kluczowych**. EE dodała komunikację elektroniczną i identyfikację cyfrową, LV bankowość i infrastrukturę rynków finansowych, a LT kilka gałęzi przemysłu oraz obronę cywilną i narodową. Kraje 3S z reguły chronią **wyższą liczbę branż** niż reszta UE. • Trzy z 28 państw członkowskich UE nie osiągnęły (stan na 24 lipca 2019) zgodności swoich przepisów dotyczących ochrony danych z zasadami unijnymi. Mimo rozpoczęcia w parlamencie procesu wdrażania **RODO** w kwietniu 2017 roku SI wciąż go nie zakończyła. • Choć nie stanowią formalnie części prawodawstwa, **strategie cyberbezpieczeństwa** mogą odzwierciedlać krajowe bądź regionalne podejście do tej kwestii. Dokumenty takie powstały w każdym z 12 omawianych krajów. • Trzecie wreszcie i najnowsze prawo przyjęte na poziomie unijnym to **akt o cyberbezpieczeństwie**, obowiązujący od czerwca 2019 roku, który uspójni wysiłki w UE i regionie.	• Ogólny stan **produkcji i zużycia energii** w krajach 3S opisuje się zazwyczaj jako mierny pod względem standardów ekologicznych. Dzieje się tak głównie za sprawą dwóch państw, PL i CZ, oraz ich historii wydobycia i spalania węgla. • W roku 2020 udział **centrów danych i sieci telekomunikacyjnych** w łącznym zużyciu energii elektrycznej w UE-28 sięgnie 3,8% w porównaniu z 2,6% w 2011. Jeśli chodzi o region EŚW w szczególności, średnią roczną stopę wzrostu samego rynku centrów danych ocenia się na 5% w okresie 2018–2024. • Podczas gdy końcowe zużycie energii w przemyśle UE-28 spadło między 2006 a 2017 o 12,8%, zużycie energii pochodzącej ze źródeł odnawialnych i biopaliw wzrosło o 28,4%. W przemyśle EŚW natomiast przyrost udziału energii ze źródeł odnawialnych i biopaliw okazał się jeszcze bardziej znaczący i osiągnął w podanych latach 50,1%. • Branżę energetyczną objęto różnymi ramami prawnymi dotyczącymi cyberbezpieczeństwa, jednak jej nietypowa natura sprawia, że istnieje tu potrzeba legislacji osobnej. W tym celu Komisja Europejska w kwietniu 2019 roku przyjęła **zalecenia na temat cyberbezpieczeństwa w energetyce**. • Region EŚW z racji **wysokiego udziału paliw kopalnych** w produkcji i zużyciu energii oraz spodziewanego **szybkiego wzrostu lokalnego sektora teleinformatycznego** powinien dokładać starań i podejmować kroki, aby zmierzać w stronę energetyki ekologicznej.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze non-profit założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz NATO. Instytut specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni.

INSTYTUT KOŚCIUSZKI