INSTYTUT KOŚCIUSZKI | BRIEF PROGRAMOWY | KWIECIEŃ 2020
ISSN 1689-9873

危机 [wēijī]

Izabela Albrycht – Prezes Zarządu, Instytut Kościuszki
Michał Kanownik – Prezes Zarządu, ZIPSEE Cyfrowa Polska
Robert Siudak – Dyrektor Niewykonawczy, Instytut Kościuszki

WSTĘP

Słowo „kryzys" w języku chińskim (危机) składa się z dwóch znaków, jeden oznaczający „zagrożenie", a drugi „szansę". Świat stanął aktualnie w obliczu zagrożenia wywołanego pandemią koronawirusa SARS-CoV-2 i choroby COVID-19, która swe początki ma w Chińskiej Republice Ludowej. Według wszelkich analiz ekonomicznych doprowadzi ona do światowej recesji, być może nawet depresji, a w konsekwencji także do przemodelowania globalnej gospodarki. Wiele wskazuje na to, że epidemia spowodowana koronawirusem będzie mniej śmiertelna niż jej wielkie poprzedniczki, hiszpanka czy dżuma, ale z całą pewnością będzie epidemią burzącą zastany porządek ekonomiczny i społeczny, z potencjalnymi reperkusjami również w wymiarze bezpieczeństwa międzynarodowego. Zgodnie z wyliczeniami brytyjskiej organizacji Henry Jackson Society, kraje grupy G7 już w tym momencie przeznaczyły 4 bln $ na wsparcie dla swoich gospodarek. Szacunki te bazują nie na zadeklarowanych, ale na formalnie ogłoszonych wydatkach na dzień 5 kwietnia 2020 r. Wielka Brytania alokowała na ten cel sumę w wysokości 449 mld $, Stany Zjednoczone – 1 200 mld $, Kanada – 59 mld $, Australia – 37 mld $[1]. Polska w ramach programu tarczy antykryzysowej przeznaczy 51,3 mld $ na wsparcie gospodarki.

1 Matthew Henderson, Dr Alan Mendoza, Dr Andrew Foxall, James Rogers, Sam Armstrong, *Coronavirus Compensation? Assessing China's Potential Culpability and Avenues of Legal Response*, https://henryjacksonsociety.org/publications/coronaviruscompensation/, [online: 5.04.2020].

W obliczu wyzwania związanego z pandemią SARS-CoV-2, obok określonych działań w zakresie zdrowia publicznego, bezpieczeństwa narodowego i polityki społecznej, Polska już teraz musi myśleć o strategii gospodarczej na przyszłość, identyfikując szanse ekonomiczne, które powstaną wraz z narodzinami nowego cyfrowego świata, który formuje się właśnie na naszych oczach.

ZARZĄDZANIE PAŃSTWEM W CZASACH KRYZYSU, TO NIE TYLKO ZARZĄDZANIE KRYZYSEM

W kontekście działań polskiego państwa priorytet numer jeden stanowi bezsprzecznie zapewnienie sprawnego funkcjonowania systemu opieki zdrowotnej oraz ograniczenie tempa rozprzestrzeniania się wirusa SARS-CoV-2 (w ramach strategii tłumienia, zorientowanej na eliminację przenoszenia choroby między ludźmi) w celu zabezpieczenia produkcji, zakupu i dystrybucji dostatecznych zasobów medycznych oraz logistycznych. Drugim kluczowym wyzwaniem jest wsparcie dla przedsiębiorców oraz pracowników, które zminimalizuje społeczne i gospodarcze skutki spowolnienia (a być może nawet zapaści ekonomicznej) w poszczególnych branżach oraz całej gospodarce. Przyjęta polityka tłumienia odciska piętno zarówno na popytowej, jak i podażowej składowej równania ekonomicznego. Zarówno w pierwszym jak i drugim kontekście politycy oraz administracja rządowa podejmują

szereg inicjatyw szeroko analizowanych wśród ekspertów, w mediach czy wśród obywateli. W Polsce już na wczesnym etapie wdrożono tzw. środki prewencyjne (ang. *non-pharmaceutical interventions*, NPI), zmierzające do ograniczenia zasięgu rozprzestrzeniania się choroby w społeczeństwie poprzez samoizolację oraz ograniczenie mobilności obywateli.

Jak pokazują badania bazujące na danych z poprzedniej wielkiej epidemii – hiszpanki z roku 1918 – takie działania wbrew pozorom mogą mieć także długookresowy sens ekonomiczny. Regiony, które szybciej wprowadziły NPI w roku 1918 szybciej były w stanie zakończyć fazę zwalczania choroby i przejść do kolejnego etapu walki ze skutkami pandemii. Ustalenia ekspertów wskazują zatem, że NPI nie tylko obniżają śmiertelność, ale pośrednio zmniejszają również negatywne skutki gospodarcze pandemii[2].

> **Celem niniejszego briefu jest zwrócenie uwagi na trzeci, niezbędny wymiar aktualnego namysłu i działań, który jest bezwzględnie konieczny na dalszym etapie walki z pandemią, a który nazwać można namysłem strategiczno-ekonomicznym i zawrzeć w pytaniu „co dalej?". W jaki sposób polskie państwo, jego gospodarka i społeczeństwo powinny rozwijać się w nowej rzeczywistości geopolitycznej i ekonomicznej, która wykrystalizuje się po aktualnym okresie kryzysu i transformacji. Wnioski wynikające z tak zadanych pytań powinny już teraz, na etapie walki z doraźnymi wyzwaniami w trakcie kryzysu epidemicznego i gospodarczego, kształtować polityki wsparcia i redystrybucji środków przez polskie państwo.**

Polskie społeczeństwo posiada nie tak odległe doświadczenie transformacji oraz kryzysu gospodarczego, który był jednym ze skutków przyjętego w 1989 r. modelu przemian. Trzydzieści lat później, posiadając rozwiniętą gospodarkę wolnorynkową, zasoby analityków zarówno w administracji publicznej, jak i ośrodkach eksperckich, a także uformowaną klasę polityczną, polskie państwo w obliczu wyzwania związanego z czasem transformacji i kryzysu musi być zdolne do namysłu, przyjęcia strategii i jej wdrażania. W pierwszym kroku powinniśmy dokonać selekcji sektorów kluczowych, które w krótkim okresie najgorszego kryzysu gospodarczego zostaną specjalnie wsparte w celu „utrzymania ich przy życiu", dzięki czemu w średnim i długim okresie, już po zapaści, staną się motorem rozwoju oraz konkurencyjności polskiej gospodarki w kolejnych dekadach XXI wieku. Naszym celem powinno być wyciągnięcie wniosków z trudnego czasu transformacji postkomunistycznej i wystrzeganie się błędów związanych z brakiem celowego działania państwa w celu ochrony oraz wsparcia sektorów kluczowych z perspektywy dalszego rozwoju naszego kraju.

Trendem obserwowanym teraz także w innych krajach jest redefinicja znaczenia m.in. takich obszarów jak służba zdrowia, produkcja przemysłowa (w tym środki ochrony osobistej i sprzęt medyczny), rolnictwo, ale także sektora technologicznego.

Trwa także namysł nad radykalnymi działaniami, które nie mieszczą się w dotychczasowych kanonach wspólnego rynku unijnego. Już dziś rząd Włoch planuje rozszerzyć swoje uprawnienia kontrolne na cały sektor bankowy i ubezpieczeniowy, a także na zdrowie i przemysł spożywczy tak, aby w czasie kryzysu zagraniczni inwestorzy, również z innych krajów Unii Europejskiej, nie mogli kupić aktywów w branżach uznanych za strategiczne dla kraju. Ceny akcji wielu spółek załamały się w związku z kryzysem epidemicznym. Dotychczas tego typu ochrona zabezpieczała przemysł obronny, energetyczny i telekomunikacyjny, a także kluczową infrastrukturę finansową i systemy płatności, jednak nie obejmowała ona krajów Unii Europejskiej[3].

Za tak postawionym dla Polski zadaniem kryje się ważne założenie co do roli i zakresu wsparcia oraz ochrony państwa w trakcie kryzysu. Wszystkie miejsca pracy są tak samo ważne z perspektywy polityki społecznej, ale nie wszystkie gałęzie gospodarki są tak samo istotne z perspektywy polityki gospodarczej państwa. O ile w tym pierwszym kontekście zadaniem rządzących jest rozciągnięcie parasola ochronnego nad wszystkimi obywatelami, o tyle w drugim państwo polskie może i powinno powiedzieć wprost – musimy **chronić** wszystkie strategiczne sektory polskiej gospodarki, ale nie stać nas, aby **wspierać** wszystkie gałęzie gospodarki równocześnie.

> **Mądra polityka gospodarcza (nie społeczna, bo nie o niej tu mowa) czasów kryzysu, musi być zdolna do strategicznej selekcji oraz alokowania środków i wsparcia dla branż oraz sektorów, które po okresie załamania rynków będą w stanie tworzyć przewagi konkurencyjne odbudowującej się gospodarki, zapewniać jej innowacyjność, wzrost produktywności i bezpieczeństwo.**

Patrząc na globalne przemiany gospodarczo-polityczne, których katalizatorem stał się także kryzys związany z pandemią SARS-CoV-2, teza jaką wysuwają autorzy niniejszego briefu jest następująca: **polskie państwo, jako jeden z sektorów kluczowych, powinno wybrać szeroko rozumiany rynek rozwiązań teleinformatycznych (ICT)**. W jego skład wchodzić powinny zarówno segmenty, takie jak gaming czy Internet Rzeczy (IoT), ale także cyberbezpieczeństwo, sztuczna inteligencja, automatyzacja produkcji, analiza Big Data oraz inne. Tak jak sektorem kluczowym dla pierwszej rewolucji przemysłowej było włókiennictwo, dla drugiej hutnictwo, dla trzeciej przemysł wytwórczy, tak szeroko

2 Sergio Correia, Stephan Luck, Emil Verner, *Pandemics Depress the Economy, Public Health, Interventions Do Not: Evidence from the 1918 Flu*, https://ssrn.com/abstract=3561560, [online: 1.04.2020].

3 *Italy plans to widen special powers over strategic sectors*, Reuters, https://www.reuters.com/article/health-coronavirus-italy-golden-powers/italy-plans-to-widen-special-powers-over-strategic-sectors-idUSL8N2BS0IU, [online: 5.04.2020].

definiowana czwarta rewolucja przemysłowa, która w XXI wieku będzie napędzać globalną gospodarkę, opiera się na sektorze ICT.

> **Ważne, aby Polska po raz kolejny nie stanowiła peryferii zmian ekonomicznych i mogła uczestniczyć w tym wyścigu, zajmując dzięki temu odpowiednio wysoką pozycję w łańcuchu wartości wytwórczej. W tym celu na etapie walki z aktualnym kryzysem gospodarczym należy wesprzeć polski sektor ICT, tak aby w kolejnych dekadach mógł stanowić silnik napędowy polskiego PKB.**

CYFRYZACJA W DOBIE KRYZYSU

Konieczne jest także zmapowanie tych sektorów, dla których warunkiem utrzymania dalszej konkurencyjności będzie gwałtowna cyfryzacja procesów zarządzania czy produkcji. Również w tym zakresie państwo nie może pozostać bierne. Wśród sektorów typowanych do głębokiej i szybkiej cyfrowej transformacji w związku z pandemią są przede wszystkim wytwórczy, bankowy, zdrowotny, transportowy[4]. Jest to szansa na to, aby tam gdzie to możliwe popyt krajowy na rozwiązania cyfrowe i z zakresu cyberbezpieczeństwa połączyć z krajową podażą. W wystąpieniu prezentującym założenia tarczy antykryzysowej w Senacie, premier Mateusz Morawiecki słusznie zaznaczył, że konieczne jest tworzenie modelu napędzania podaży krajowej przez popyt. W przypadku wsparcia dla szeroko rozumianego sektora technologicznego, w tym cyberbezpieczeństwa, rozwiązanie to wydaje się mieć szczególne zastosowanie.

> **Pomimo kryzysu przyspieszy także proces budowy nowoczesnej infrastruktury telekomunikacyjnej, w tym sieci nowej generacji – 5G. Kwestia ta, choć w wyniku pandemii nie jest już na pierwszych stronach gazet, to wciąż jest jednym z najważniejszych wyzwań współczesnych krajów i w jeszcze większym stopniu wpłynie na ich konkurencyjność po epidemii.**

W USA firmy AT&T i Verizon oświadczyły już, że większość swoich środków na inwestycje przeznaczą na rozbudowę sieci internetowej, wskazując nie tylko na zwiększone zapotrzebowania na przesył danych w wyniku zmiany w kulturze pracy i spędzania wolnego czasu, ale także na potrzebę zapewnienia firmom dobrej pozycji gdy minie pandemia, a gospodarka zacznie się odbijać[5]. W tym kontekście prace nad rozwojem sieci 5G w Polsce ze wsparciem państwa powinny znacząco przyspieszyć. Zwłaszcza, że 5G będzie napędzało gospodarkę cyfrową, generując nowe miejsca pracy i stymulując wzrost gospodarczy. Zgodnie z najnowszymi danymi GSMA oczekuje się, że technologia 5G wniesie do światowej gospodarki 2,2 bln $ w perspektywie 2034 roku[6].

Jednocześnie w związku ze zwiększającą się liczbą ataków cyfrowych powinniśmy wziąć po uwagę potrzebę budowy nie tylko sieci efektywnej, ale i odpornej na zagrożenia. Z tego względu, jak wielokrotnie wskazywaliśmy w naszych analizach, należy korzystać z zaufanych dostawców technologii[7]. Teraz ważniejsze niż kiedykolwiek wcześniej będzie zrozumienie, że własne cyfrowe zasoby technologiczne, również w sektorze cyberbezpieczeństwa oraz 5G, a także lokowanie w Polsce działalności naukowo-badawczej i fabryk firm ICT, są podstawą budowy bazy technologicznej oraz zasobów kompetencji w gospodarce, umożliwiających zabezpieczenie funkcjonowania państwa w XXI wieku.

Należy w związku z tym podjąć wysiłek i działania zmierzające do wspierania zwłaszcza tych dostawców technologii 5G, którzy zakorzenieni są w Europie. W następnej perspektywie finansowej Unii Europejskiej należy położyć nacisk na to, aby to oni uczestniczyli w budowie sieci 5G w Europie. Także dlatego, że w tym roku obserwujemy silny trend, w którym rynek chiński jednoznacznie preferuje dostawców chińskich, prawdopodobnie także jako odpowiedź na ekonomiczne skutki pandemii, ale przede wszystkim dlatego, że bezpieczeństwo swej sieci, postrzega jako potrzebę powierzenia go firmom, którym ufa. Niedawno Huawei i ZTE wygrały przetarg giganta telekomunikacyjnego China Mobile na budowę sieci 5G w zakresie 90% zapotrzebowania na technologię[8]. Podobnie powinni działać Europejczycy dostrzegając zarówno szanse, jak i zagrożenia związane z budową sieci nowej generacji.

> **Z całą pewnością pandemia pozostawi świat bardziej cyfrowym niż zastała, a takie trendy jak gospodarka oparta na danych czy automatyzacja nie będą w przeważającej mierze już tylko konceptem, ale staną się naszą rzeczywistością. Im szybciej tę wiedzę zakumulujemy na wszystkich poziomach zarządzania państwem i gospodarką, tym lepiej. Jednocześnie zaadresować będzie trzeba także skutki dla tych modeli ekonomicznych, które w wyniku pandemii mogą się okazać zagrożone, jak np. ten popularny od czasów poprzedniego kryzysu finansowego, a mianowicie model ekonomii współdzielenia.**

4 O zastosowaniu do niektórych z nich technologii sztucznej inteligencji Instytut Kościuszki pisał w raporcie pt. *Sztuczna Inteligencja – AI made in Asia*, zobacz więcej: https://ik.org.pl/publikacje/sztuczna-inteligencja-made-in-asia/, [online: 5.04.2020].

5 John Hendel , *After the virus: A 5G gold rush?*, https://www.politico.com/news/2020/04/02/coronavirus-5g-network-160296, [online: 5.04.2020].

6 *The Mobile Economy 2020*, GSMA, https://www.gsma.com/mobileeconomy/?utm_source=Organic_Social&utm_medium=Twitter&utm_campaign=Mobile_Economy_Report_2020, [online: 5.04.2020].

7 Izabela Albrycht, dr Joanna Świątkowska, *Przyszłość 5G czyli Quo Vadis, Europo?*, https://ik.org.pl/publikacje/przyszlosc-5g-czyli-quo-vadis-europo-2/, [online: 4.04.2020].

8 Izabela Albrycht, *Koronawirus pozwala się mnożyć wirusowi cyberzagrożeń. Jak chronić się przed atakami?*, https://biznesalert.pl/izabela-albrycht-koronawirus-cyberbezpieczenstwo-praca-zdalna-5g-cyberprzestrzen/, [online: 4.04.2020].

KONIEC GLOBALIZACJI JAKĄ ZNAMY

Punktem wyjścia do tej analizy powinien być wskazany już fakt, że w tle walki z COVID-19 coraz szybciej postępują zmiany w globalnym systemie, które rozpoczęły się w związku z nasilającą się rywalizacją strategiczną Stanów Zjednoczonych i Chińskiej Republiki Ludowej, a przejawiają się przede wszystkim w dynamicznym procesie rozrywania globalnych łańcuchów dostaw (ang. *decoupling of global supply chains*). W toku tych przemian obserwujemy ruchy chińskich podmiotów, aby zdobyć jak największą przestrzeń do dalszej obecności biznesowej w Europie. Nasz kontynent jest obszarem szczególnie istotnym w świetle tej rywalizacji.

Aby zdyskontować kryzys poszczególne kraje i UE *en bloc*, tworząc własne strategie walki z pandemią, muszą przyjąć założenie, że konieczne jest alokowanie zasobów w te obszary gospodarki, które zapewnią najlepszą stopę zwrotu gospodarczego i społecznego, a jednocześnie wspierać będą budowę autonomii strategicznej w każdym kluczowym wymiarze, który dotknięty zostanie także skutkami *decouplingu*. Proces ten jest szczególnie widoczny w ramach cyfrowego łańcucha dostaw.

> **W nowym świecie wymiar cyfrowy okazuje się już teraz być krytycznie istotny z punktu widzenia ciągłości biznesowej, jak i funkcjonowania państwa. Jeśli jeszcze ktokolwiek w to wątpił, to z pewnością już dziś dostrzega, że technologia ma narodowość i posiadanie stabilnych oraz niezakłóconych usług telekomunikacyjnych i informatycznych, a także bezpiecznego łańcucha dostaw w sektorze ICT jest koniecznością.**

Na zagadnienie to w kontekście wymiaru cyfrowego zwracała uwagę Komisja Europejska w publikacji *Rethinking Strategic Autonomy in the Digital Age*[9] pisząc, że „w XXI wieku ci, którzy kontrolują cyfrowe technologie, mają coraz większy wpływ na wyniki gospodarcze, społeczne i polityczne. Decydenci polityczni na całym świecie budzą się i zaczynają rozumieć krytyczny wpływ, jaki cyfrowe technologie mają na strategiczną autonomię ich krajów i globalny wyścig o wiodącą pozycję technologiczną. Mimo wielu atutów, które posiada UE, istnieje zagrożenie, że w tym wyścigu pozostanie ona w tyle. Nie tylko zagraża to jej długoterminowemu dobrobytowi gospodarczemu, ale także otwiera ją na całą gamę strategicznych słabości – tym bardziej, że wyścig ten odbywa się na tle eskalacji napięć geopolitycznych". Tzw. geopolityczna Komisja Europejska, której kadencja rozpoczęła się w listopadzie 2019 roku, położyła bardzo duży nacisk na strategię cyfrową dla Europy. W obliczu dokonującej się w czasach pandemii gwałtownej transformacji cyfrowej można się spodziewać, że działania w zakresie budowania suwerenności cyfrowej zostaną zintensyfikowane. Polska powinna w tym zakresie ściśle współpracować z pozostałymi krajami unijnymi.

Globalne firmy technologiczne, które stały się w tych dniach *de facto* tzw. *public utilities* i są już na stałe wpięte w system społeczno-ekonomiczny krajów i międzynarodowych instytucji, zdały w ostatnich dniach test z niezawodności i odpowiedzialności. Będą one prawdopodobnie też tymi podmiotami, z którymi kryzys obejdzie się najłaskawiej. Zapotrzebowanie na ich usługi nie zmaleje, a wzrośnie, zaś same firmy zostaną równoprawnymi partnerami dla krajów narodowych w adresowaniu globalnych wyzwań. W globalnym wyścigu technologicznym najważniejszą przewagą będzie jednak zwinność i innowacyjność. Dlatego kluczowe stanie się wspieranie przez poszczególne państwa, ale także gigantów technologicznych, rozwoju tego sektora firm ICT i cyberbezpieczeństwa, które inwestują znaczące środki w rozwój własnych produktów oraz badania i rozwój (narodowi czempioni i MŚP), jak i proponują przełomowe rozwiązania, które jednak dla rynku mogą wiązać się z pewnym początkowym ryzykiem inwestycyjnym (start-upy).

W kontekście Europy Środkowo-Wschodniej ważne jest kontynuowanie propozycji zarysowanych w koncepcji Cyfrowego Trójmorza, które pozwolą na realizację przytoczonych powyżej kluczowych celów[10]. Region po analizie swoich przewag konkurencyjnych musi także podjąć działania zmierzające do wykorzystania szansy jaką niesie ze sobą *decoupling*, a wraz z nim rosnące prawdopodobieństwo przenoszenia zagranicznych inwestycji w sektorze nowoczesnych technologii z Chin w inne miejsca świata[11], a także przenoszenia stamtąd produkcji, z czasem coraz bardziej zautomatyzowanej, w inne rejony świata.

W Europie musimy rozumieć sytuację kryzysową, w której się znaleźliśmy tak, jak rozumieją ją Chińczycy – jako niebezpieczeństwo, z którego jednak wyłaniają się nowe możliwości, w tym przypadku cyfrowe.

CYBERWIRUS

Kolejną zmienną, którą należy podnieść w kontekście rosnącego znaczenia firm technologicznych, jest aktualnie obserwowana epidemia cyberzagrożeń. Jej zasięg zwiększa się wraz z szerzeniem się na świecie wirusa SARS-CoV-2. Choć należy ją postrzegać jako pośrednią konsekwencję pandemii, to jednak jej koszty będą bezpośrednio wpływać na kondycję światowej gospodarki i to w większym niż

9 Komisja Europejska, *Rethinking Strategic Autonomy in the Digital Age*, https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf, [online: 28.03.2020].

10 Inicjatywa opisana jest na stronie internetowej Inicjatywy Cyfrowego Trójmorza: https://digital3seas.eu/.

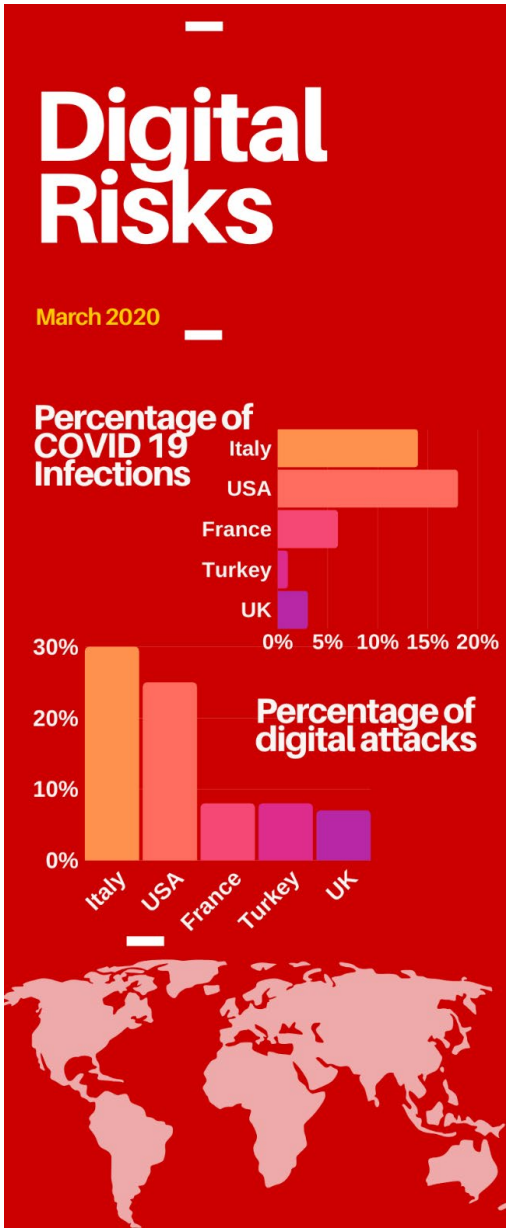
11 Izabela Albrycht, *Cyfrowa Zimna Wojna*, https://www.forbes.pl/opinie/cyfrowa-rywalizacja-miedzy-usa-a-chinami-komentarz-instytutu-kosciuszki/7kh4nhv, [online 28.03.2020].

dotychczas wymiarze. Już teraz widzimy wzrost liczby ataków w cyberprzestrzeni, zarówno tych wymierzonych w indywidualnych użytkowników (głównie pracujących w trybie *home office*), jak i w organizacje mierzące się z klęską pandemii na pierwszym jej froncie (ośrodki medyczne). Innymi słowy, w czasie kiedy nasza uwaga skupiona jest na walce na froncie biologicznym, na tym cyfrowym toczy się coraz bardziej zaciekła walka dobra ze złem. Kiedy prywatni użytkownicy Internetu korzystają z globalnej sieci, urządzeń, oprogramowania i aplikacji, aby kontynuować swoją działalność biznesową, komunikować się z przyjaciółmi i rodziną, kupować produkty i usługi, to cyberprzestępcy szukają podatności w systemach i urządzeniach, z których korzystamy, próbując ukraść nasze dane, tożsamość czy pieniądze. Nasza aktywność online rośnie, ich również.

Jednocześnie zdaniem firmy SecDev Group widoczna jest bezpośrednia korelacja między liczbą infekcji w danym kraju a wzrostem zagrożeń w cyberprzestrzeni i ataków cyfrowych. Przyrostowi zachorowań we Włoszech, USA i Francji towarzyszy wzrost ataków w cyberprzestrzeni, zwiększając znacząco profil ryzyka cyfrowego w tych krajach (zobacz Grafika 1). Widzimy też, że nastąpił znaczny wzrost liczby złośliwych ataków zawierających oprogramowanie *ransomware* na obiekty medyczne. Cyberprzestępcy zalewają nimi szpitale, laboratoria medyczne, zakłady testowania szczepionek i dostawców usług krytycznych wyłudzając informacje i zmuszając niektórych do zamknięcia. Do takich ataków doszło już w Stanów Zjednoczonych, Hiszpanii, Wielkiej Brytanii i Francji. Inne formy ataków przywołane przez SecDev, to m.in. ataki *phishingowe* na firmy i administrację rządową zmuszoną do szybkiego przeniesienia pracy biurowej do domów, gdzie pracownicy nie korzystają z odpowiedniej architektury bezpieczeństwa sieci i urządzeń końcowych. Zagrożenie stanowią także złośliwe aplikacje i fałszywe witryny oferujące mapy i analizy dot. rozprzestrzeniania się COVID-19, które mogą wykraść dane uwierzytelniające użytkowników.

Dane przedstawione przez SecDev wskazują, że domeny związane tematycznie z pandemią COVID-19 są o 50% bardziej podatne na złośliwe oprogramowanie, niż inne domeny zarejestrowane w tym samym okresie. Na ataki szczególnie narażone są jednak poszczególne sektory gospodarki oraz instytucje znajdujące się na pierwszym froncie walki z epidemią. Dzieje się tak gdyż ich pracownicy aktywnie poszukując informacji na temat COVID-19, częściej klikają złośliwe linki lub załączniki, co czyni ich atrakcyjnymi celami dla hakerów. Do takich podmiotów należą szpitale oraz inne instytucje służby zdrowia i epidemiologiczne, a także administracja rządowa i samorządowa, ośrodki edukacyjne i placówki naukowo-badawcze.

Grafika 1.



źródło: SecDev Group

> **Firmy zajmujące się cyberbezpieczeństwem zidentyfikowały kilka podmiotów aktywnie angażujących się w cyberoperacje powiązane z pandemią SARS-CoV-2. Ich zdaniem niektóre z tych podmiotów mogą być sponsorowane przez państwa. Są nimi m.in. Grupa Hades, działająca poza Rosją z powiązaniami z APT28 (Fancy Bear), chińska Mustang Panda czy pakistańska APT36.**

W tej sytuacji konieczna jest mobilizacja po obu stronach – firmy i instytucje narażone na cyberataki muszą wdrażać bezpieczne rozwiązania i procedury, z kolei firmy oferujące rozwiązania bezpieczeństwa dla sieci i systemów ICT muszą się zmobilizować do współpracy z instytucjami publicznymi i krytycznymi sektorami gospodarki, a w ramach sektorowej współpracy wymieniać informacjami i *know how*.

Jednocześnie, mimo że globalne firmy technologiczne wykazują się w czasie pandemii dużą odpowiedzialnością za bezpieczeństwo transformacji cyfrowej, to jednak jest to dla nich czas wzmożonej czujności i wytężonych działań, które powinny zmierzać do wpisania bezpieczeństwa w DNA urządzeń, systemów, oprogramowania, aplikacji, platform do komunikacji i pracy zbiorowej oraz wielu innych cyfrowych udogodnień. Problem z bezpieczeństwem i prywatnością w ramach korzystania z platformy ZOOM jest tego dobitnym przykładem.

W kontekście zagrożeń dla bezpieczeństwa sieci należy także postrzegać w tych dniach kwestię wzmożonego ruchu i potencjalne problemy z przepustowością sieci internetowej. Operatorzy sieci telekomunikacyjnych i dostawcy Internetu stali się w tej sytuacji krytycznym zasobem państwa, od którego zależy płynność działalności biznesowej i praca administracji publicznej. Dlatego już dziś należy podjąć kroki zmierzające do rozbudowy sieci internetowej w Polsce, na co zwróciliśmy już uwagę w poprzedniej części publikacji.

KRYZYS A DYNAMIKA RYNKU ICT

Kryzys epidemiczny zmusił wiele branż do gwałtownej transformacji cyfrowej związanej z potrzebą pracy zdalnej oraz digitalizacji kluczowych procesów. Jesteśmy świadkami ekspresowego procesu edukacji, w praktyce całego rynku i społeczeństwa, w zakresie potrzeb cyfrowych. Obserwujemy także wzrost zagrożeń dla bezpieczeństwa sieci i systemów informatycznych.

W średnio i długookresowym scenariuszu przełoży się to na zwiększone zapotrzebowanie zarówno na usługi, jak i produkty ICT oraz cyberbezpieczeństwa na świecie i w Polsce. Jednocześnie w krótkim okresie, zapewne co najmniej do Q1 2021, rynek w odpowiedzi na szok popytowy oraz podażowy ograniczy zakup rozwiązań, co może zagrozić wręcz wyeliminowaniem z rynku i upadłością całego segmentu polskich MŚP/startupów z sektora ICT, które w ogromnej większości nie posiadają rezerw kapitałowych, aby przetrwać takie spowolnienie.

Ten negatywny scenariusz oznaczać będzie, że podmioty z rynków nasyconych kapitałowo, które posiadają rezerwy, przetrwają kryzys, a następnie w średnim i długim okresie (Q4 2021, 2022/2023) zdyskontują i zmonetyzują zapotrzebowanie globalnej i polskiej gospodarki na rozwiązania ICT i cyberbezpieczeństwa, także dzięki brakowi konkurencji z rynków regionalnych, w znacznej mierze przetrzebionych przez kryzys. Aby temu zaradzić niezbędne jest celowe działanie państwa, również we współpracy z większymi firmami z branży ICT. Jednocześnie w czasie kryzysu epidemicznego, idąc za przykładem innych państw, rząd i służby bezpieczeństwa powinny wspierać budowę cyberkoalicji firm prywatnych i współpracować z nimi. Takie koalicje pojawiły się ochotniczo np. w Kanadzie - COVID-19 Cyber Defense Force, która zapewnia szpitalom, gminom i krytycznej infrastrukturze pełny pakiet usług w zakresie cyberbezpieczeństwa[12]. Podobne cele przyświecają w Stanach Zjednoczonych Covid-19 CTI League i brytyjskiej CV19, które koncentrują się na profilaktyce i reagowaniu na zagrożenia w sektorze opieki zdrowotnej, który jest szczególnie wrażliwy i krytycznie zagrożony atakami[13].

POTRZEBNE DZIAŁANIA KRAJOWE

W praktyce, wskazać można co najmniej **5 propozycji celowego wsparcia dla sektora ICT i cyberbezpieczeństwa w Polsce** w kolejnych miesiącach, które powstały po konsultacji z firmami skupionymi w inicjatywie Instytutu Kościuszki, wspieranej przez ZIPSEE, pod nazwą #CyberMadeInPoland[14]:

1. „Pożyczki technologiczne" lub inwestycje bezpośrednie realizowane przez Polski Fundusz Rozwoju lub Bank Gospodarstwa Krajowego.

Niskooprocentowane lub bezzwrotne pożyczki ekspresowe z przeznaczeniem dla MŚP i startupów, udzielane w zależności od oceny wartości biznesowej usługi lub produktu z kluczowego sektora. Zwrot niskooprocentowanej pożyczki następowałby w wypadku uzyskania przez tę firmę przychodów powyżej danego pułapu w określonym horyzoncie czasowym (np. Q4 2021). Jeśli sytuacja taka nie miałaby miejsca pożyczka staje się bezzwrotną (reguła wykorzystywana w wielu krajach w odniesieniu do kredytów na studia). Dla polskich firm z branży cyberbezpieczeństwa, w przypadku ich wyjścia na rynki zagraniczne, należałoby także opracować dedykowaną ofertę wsparcia ubezpieczeniowego i inwestycyjnego w ramach Korporacji Ubezpieczeń Kredytów Eksportowych.

Operatorzy funduszy rozwojowych, w ramach działań antykryzysowych, powinni również rozważyć możliwość pośredniego wejścia kapitałowego, wykupu udziałów, w przypadku zainteresowanych firm z rodzimego sektora ICT i cyberbezpieczeństwa.

2. Wsparcie w modelu popyt-podaż:
    a. Promocja systemowa podmiotów MŚP/startupów w ramach digitalizacji administracji publicznej.

12 Więcej o COVID-19 Cyber Defense Force: https://www.cisomag.com/canadas-cyber-defense-and-world-cti-league-fight-against-covid-19-cyberattacks/?utm_source=Rafal+AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, [online: 6.04.2020].

13 więcej o Covid-19 CTI League i brytyjskiej CV19: https://www.sdxcentral.com/articles/news/security-experts-battle-hackers-covid-19-cyberattacks/2020/03/?utm_source=Rafal+AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, https://cyberv19.org.uk/?utm_source=Rafal%20AUDIENCE&utm_campaign=d5b59784b1-Covid19-John-Contacts-March-1_COPY_01&utm_medium=email&utm_term=0_6e92156d31-d5b59784b1-395352172, [online: 6.04.2020].

14 Podobne wnioski zostały przedłożone Radzie do spraw Cyfryzacji przy Ministerstwie Cyfryzacji, która podjęła pracę nad *Stanowiskiem w sprawie wsparcia polskiego sektora ICT w kontekście działań antykryzysowych* zawartym w Uchwale nr 4 Rady: https://www.gov.pl/web/cyfryzacja/dokumenty-rady-kadencji-2019-2021, [online: 16.04.2020].

Działanie wspierające może przyjąć wiele form, w tym np. ustanowienia specjalnych pozacenowych kryteriów w postępowaniach publicznych, promujących rozwiązania oferowane przez firmy polskiego pochodzenia (spełnienie kryteriów daje oferentowi dodatkowe punkty w postępowaniu, ale nie wprowadza preferowania określonych podmiotów, aby uniknąć zarzutu ograniczenia konkurencyjności), czy też wprowadzenie pewnych wymagań systemowych, takich jak potrzeba uzyskania zawsze wyceny od polskiego MŚP w procesie zamówienia publicznego. Innym działaniem może być zobligowanie określonych podmiotów odpowiedzialnych za cyfryzację sektora publicznego – np. COI, NASK – do współpracy z segmentem MŚP/startupy. Innym pomysłem opracowanym przez Ministerstwo Cyfryzacji są tzw. publiczne roboty cyfrowe, które mają umożliwić firmom udział w procesach związanych z informatyzacją administracji publicznej. Jest to rozwiązanie, które ma większą wartość dodaną niż transfer środków pomocowych na funkcjonowanie tychże firm.

b. W średnim okresie wsparcie poprzez stymulację strony popytowej w zakresie digitalizacji tradycyjnych gałęzi gospodarki.

Państwo do stymulowania popytu posiada szereg narzędzi, w tym m.in. ulgi podatkowe czy programy dedykowane zakupom z zakresie zapotrzebowania na określone rozwiązania. Przykładowym działaniem, z jednej strony zapewniającym bezpieczeństwo transformacji cyfrowej w kraju, z drugiej wspierającym krajowy rynek cyberbezpieczeństwa, może być kwalifikowanie wydatków na cyberbezpieczeństwo jako wydatków na innowacje (utworzona mogłaby zostać dedykowana ulga inwestycyjna dla wydatków na *cybersecurity*), co wiązałoby się z odpisami CIT, rozszerzeniem stosowania „Innovation BOX" poprzez zwiększenie poziomu obniżenia poziomu opodatkowania dochodu uzyskiwanego z praw własności intelektualnej do 10 % oraz poszerzeniem zakresu przedmiotowego o koszty wytworzenie produktów z zakresu cyberbezpieczeństwa.

Pożądanym działaniem byłoby także uruchomienie programu „bonów na cyberbezpieczeństwo", a więc funduszy publicznych dostępnych dla jednostek samorządowych na zakup usług lub rozwiązań z zakresu bezpieczeństwa ICT przygotowanych dla nich przez polskie firmy lub jednostki badawcze.

3. Wsparcie działalności badawczo-rozwojowej poprzez natychmiastowe zwiększenie poziomów dofinansowania w ramach już trwających oraz planowanych projektów.

Narodowe Centrum Badań i Rozwoju, Polska Agencja Rozwoju Przedsiębiorczości i Agencja Rozwoju Przemysłu oraz inne agencje i instytucje powinny przeformułować reguły zarówno pomocy *de minimis* jak i pomocy publicznej dla sektorów kluczowych, w tym przede wszystkim cyberbezpieczeństwa i ICT.

Zwiększone powinny zostać poziomy dofinansowania, w zależności od wielkości firmy, nawet do 90 – 100% w przypadku MŚP i startupów. Co prawda w sytuacji niezwiększenia alokowanych środków na określone programy B+R, mniej projektów otrzyma wsparcie, ale zostanie dzięki temu zrealizowany inny kluczowy cel, czyli utrzymanie płynności realizacji projektów. Jeśli takie działania nie zostaną podjęte zagrożona będzie realizacja już funkcjonujących projektów (co oznaczać będzie zmarnotrawienie wydanych do tej pory milionów złotych) oraz zainteresowanie kolejnymi naborami (a w konsekwencji spadek innowacyjności polskiego sektora). Firmy realizujące projekty, ze względu na zapaść na rynku, już teraz, nie cały miesiąc od początku kryzysu związanego z COVID-19, napotykają problemy w znalezieniu środków na dokończenie projektów B+R. W najbliższych miesiącach nie będą zapewne w stanie wygenerować z rynku funduszy, aby kontrybuować na poziomie 80 czy 40% do trwających projektów B+R. Aby zaadresować ten problem niezbędna jest interwencja państwa, która zmieniłaby reguły ich finansowania.

4. Wsparcie w formie wprowadzenia alternatywnych sposobów ewaluacji firm aplikujących o fundusze unijne.

Ocena celowości wsparcia przedsiębiorstwa w oparciu o jego sprawozdania finansowe z ostatniego roku (lub 3 lat) w scenariuszu głębokiego kryzysu gospodarczego stanie się fikcją. Sprawozdanie takie, ze względu na szersze makroekonomiczne uwarunkowania, w wielu przypadkach nie będzie odzwierciedlać wartości firmy lub pomysłu technologicznego. W związku z tym w ramach kolejnej perspektywy finansowej UE, której realizacja rozpoczynać będzie się w okresie znacznego spowolnienia ekonomicznego, należy umożliwić alternatywne formy oceny przedsiębiorstw aplikujących o wsparcie z programów unijnych w tym regionalnych programów operacyjnych. Mogą one czerpać z metodologii stosowanej przez programy inkubacyjne lub akceleracyjne – np. ocena panelu ekspertów w zakresie wartości biznesowej rozwiązania czy technologii.

DZIAŁANIA W REGIONIE TRÓJMORZA

> **Trwająca pandemia jest także najwyższym czasem na to, aby region Europy Środkowo-Wschodniej (CEE) rozpoznał i zaadaptował się do zmian, jakie dla globalnej gospodarki przynosi niebywale gwałtowna transformacja cyfrowa w połączeniu ze zmianami geopolitycznymi i geoekonomicznymi. Proces ten należałoby rozpocząć od ambitnego rozwoju infrastruktury cyfrowej, w tym od budowy połączenia światłowodowego z USA w ramach realizacji zaproponowanej przez Exatel koncepcji transatlantyckiego kabla *„3Seas1Ocean"*, a następnie koncepcji Instytutu Kościuszki, czyli cyfrowej autostrady Trójmorza (ang. *3 Seas Digital Highway*, 3SDH) – jednego ze strategicznych projektów w ramach Inicjatywy Cyfrowego Trójmorza[15].**

15 Wpisana na listę priorytetowych projektów na Szczycie krajów Trójmorza w Bukareszcie w 2018 roku. 3SDH wypełnia luki w światłowodowej infrastrukturze telekomunikacyjnej z północy na południe regionu. Tę międzynarodową infrastrukturę cyfrową, która uzupełniona mogłaby zostać także o technologię 5G, należy wdrożyć wraz z zaplanowanymi już projektami transportowymi Trójmorza (np. Via Carpatia).

Rozwój infrastruktury cyfrowej jest nie tylko konieczny w świetle dalszego wzrostu zapotrzebowania na przesył danych, ale także dlatego, że wspierać może rozwój w regionie gospodarki cyfrowej i zachęcać firmy do podejmowania decyzji inwestycyjnych w zakresie budowy *data centers* czy relokacji centrów naukowo-badawczych. Realizacja wspólnych projektów infrastrukturalnych powinna odbywać się równolegle do rozwoju inicjatyw związanych z nowoczesnymi technologiami, szczególnie w tych sektorach, gdzie to dane są najważniejszą walutą, jak np. w usługach opartych na technologii chmury obliczeniowej, Internecie Rzeczy, sztucznej inteligencji czy centrach e-commerce. W ramach istniejącego już Funduszu Trójmorza utworzony mógłby zostać także specjalny Fundusz VC, którego celem byłoby wsparcie podmiotów sektora ICT z regionu oraz wsparcie inwestycyjne projektów z kluczowych sektorów.

Jednocześnie można sięgnąć do opisywanych już w 2019 roku propozycji, aby w związku z przewidywanymi geopolitycznymi i technologicznymi zmianami tak ukierunkować potencjał regionu CEE, aby przyciągnął on zagraniczne inwestycje w sektorze nowoczesnych technologii. „To pomogłoby krajom regionu dokonać cywilizacyjnego skoku. Zagrożenie w postaci stagnacji gospodarczej, tzw. pułapki średniego dochodu, mogącej uniemożliwić krajom CEE nadrobienie gospodarczych zaległości może zostać ostatecznie zażegnane dzięki innowacyjności i zwinności gospodarek. Rozwój nowoczesnych technologii cyfrowych może być ważną siłą napędową wzrostu gospodarczego. Dlatego jednym ze strategicznych celów regionu powinno być wspinanie się po szczeblach globalnego łańcucha dostaw w sektorze IT oraz cyberbezpieczeństwa, a także dostarczanie produktów i usług o dużej wartości dodanej. W związku z tym, aktualnym wyzwaniem dla krajów Trójmorza jest opracowanie i realizacja strategii rozwoju ukierunkowanych nie tylko na konwergencję, ale także na wysoką innowacyjność, a także na stworzenie równowagi między rozwojem przemysłu tradycyjnego a inwestycjami w przemysł nowoczesnych technologii.

> **Region CEE ma olbrzymi potencjał kompetencji cyfrowych koniecznych do wsparcia rozwoju nowych technologii takich jak sztuczna inteligencja, Internet rzeczy czy robotyzacja i automatyzacja. Aby można było je zrealizować konieczne jest systemowe wsparcie rozwoju wykwalifikowanych specjalistów oraz programów przekwalifikowania zawodowego, edukacji opartej na danych i rozwój szeroko-pojętych kompetencji cyfrowych społeczeństwa. Rozpoznanie potencjalnych przewag konkurencyjnych i dynamicznie rozwijających się nisz produktowych może pomóc CEE w staniu się jednym z liderów wyścigu technologicznego i dzięki temu w zajęciu lepszej pozycji w globalnym łańcuchu wartości”[16].**

16 Izabela Albrycht, *Cyfrowa Zimna Wojna*, https://www.forbes.pl/opinie/cyfrowa-rywalizacja-miedzy-usa-a-chinami-komentarz-instytutu-kosciuszki/7kh4nhv, [online 28.03.2020].

ZAKOŃCZENIE

Już przed pandemią COVID-19 obserwowaliśmy zmiany w potencjale projekcji siły – *soft* i *hard power*, na które coraz większy wpływ mają współczesne technologie. Technologie cyfrowe stały się bardzo ważnym czynnikiem decydującym o pozycji geopolitycznej i ekonomicznej poszczególnych krajów. W coraz większym zakresie warunkują one bowiem ich potencjał, zarówno w obszarze obronnym, jak i gospodarczym. Poszczególne kraje zaczynają rozumieć krytyczny wpływ, jaki cyfrowe technologie mają na strategiczną autonomię ich krajów i stawkę w globalnym wyścigu o wiodącą pozycję technologiczną. Odzwierciedla się to w ich strategiach, regulacjach, zachętach i decyzjach inwestycyjnych firm. Z powodów opisanych w niniejszej publikacji polskie państwo, jako jeden z sektorów kluczowych, powinno wybrać szeroko rozumiany rynek rozwiązań teleinformatycznych, w tym cyberbezpieczeństwa jako jeden z głównych filarów wzrostu gospodarczego. Strategicznym wyzwaniem będzie zatem umiejętne i mądre wsparcie rodzimego sektora ICT i cyberbezpieczeństwa w czasie pandemii SARS-CoV-2 i tzw. „cyberwirusa” oraz spodziewanego kryzysu gospodarczego, a także wprzęgnięcie tych działań w unijne tryby. Te kraje, które zrozumieją i przekują na strategię wyjścia z gospodarczego i finansowego kryzysu zarysowane szanse i zagrożenia, wyjdą z niego szybciej i będą miały większe możliwości budowania swojej pozycji w regionie, a w przypadku mocarstw, na świecie.

> **Pamiętając ambitne projekty gospodarcze II Rzeczpospolitej, która odpowiadając na wielki kryzys lat 30 XX wieku, była w stanie zapoczątkować program budowy fabryk, hut, zakładów metalurgicznych i przetwórczych w ramach Centralnego Okręgu Przemysłowego, nie bójmy się odważnych wizji w ciężkich czasach. W odpowiedzi na wyzwania związane z kryzysem ekonomicznym po pandemii SARS-CoV-2, państwo polskie musi stworzyć odpowiedni program rozwoju sektorów kluczowych dla gospodarki XXI wieku, w tym szczególnie sektora technologii cyfrowych.**

Nie mamy tu jednak na myśli próby budowania państwowych molochów, ale efektywną współpracę z sektorem prywatnym, w którym tkwi zarówno kapitał wiedzy, doświadczenie, jak i nierzadko znajomość międzynarodowych dobrych praktyk w zakresie takiej kooperacji.

INSTYTUT KOŚCIUSZKI

Instytut Kościuszki jest niezależnym, pozarządowym instytutem naukowo-badawczym (Think Tank) o charakterze non profit, założonym w 2000 r. Misją Instytutu Kościuszki jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski jako aktywnego członka Unii Europejskiej oraz partnera sojuszu euroatlantyckiego. Instytut Kościuszki pragnie być liderem pozytywnych przemian, tworzyć i przekazywać najlepsze rozwiązania, również na rzecz sąsiadujących krajów budujących państwo prawa, społeczeństwo obywatelskie i gospodarkę wolnorynkową.
Instytut Kościuszki jest organizatorem Europejskiego Forum Cyberbezpieczeństwa CYBERSEC oraz Polskiego Forum Cyberbezpieczeństwa – pierwszych w Polsce oraz jednych z nielicznych w Europie corocznych konferencji poświęconych strategicznym wyzwaniom płynącym z cyberprzestrzeni i dotyczących cyberbezpieczeństwa. Więcej: http://cybersecforum.eu/.
Instytut Kościuszki jest wydawcą „European Cybersecurity Journal" (ECJ). ECJ to anglojęzyczny kwartalnik ekspercki poświęcony cyberbezpieczeństwu. Zawiera artykuły wiodących analityków i liderów opinii, ekskluzywne wywiady z decydentami oraz monitoring regulacji dotyczących kluczowych aspektów związanych z cyberprzestrzenią. Więcej: http://cybersecforum.eu/czym-jest-ecj/.
Biuro w Krakowie: ul. Feldmana 4/9, 31-130 Kraków, Polska, tel.: +48 12 632 97 24,
www.ik.org.pl, e-mail: instytut@ik.org.pl

CYFROWA POLSKA

Związek Cyfrowa Polska to branżowa organizacja pracodawców o charakterze non-profit, reprezentująca polską branżę cyfrową i nowoczesnych technologii. Zrzesza największe firmy z branży RTV i IT działające w Polsce. To zarówno producenci, importerzy jak i dystrybutorzy sprzętu elektrycznego i elektronicznego. Organizacja działa m.in. na rzecz cyfryzacji polskiej gospodarki oraz społeczeństwa angażując się w stanowienie przyjaznego prawa dla rozwoju tego segmentu oraz działania edukacyjne zwiększające wiedzę o nowoczesnych technologiach.

#CyberMadeInPoland

Z inicjatywy Instytutu Kościuszki powstała specjalna grupa robocza *#CyberMadeInPoland* działająca przy Związku Cyfrowa Polska. Jej celem jest wspieranie rozwoju sektora cyberbezpieczeństwa w Polsce, a w jej skład wchodzą zarówno firmy wytwarzające produkty i usługi dla bezpieczeństwa cyfrowego, jak i organizacje otoczenia biznesu zajmujące się tą tematyką. Głównym zadaniem zespołu jest zainteresowanie tematyką bezpieczeństwa cyfrowego zarówno firmy działające w Polsce, jak i samorządy oraz podmioty administracji publicznej. *Inicjatywa wpisuje się w szerszy unijny kontekst dążenia do budowania „cyfrowej niezależności" Europy.*
Grupa *#CyberMadeInPoland* będzie również pracować nad stworzeniem specjalnego funduszu celowego na ekspansję zagraniczną polskich firm z branży cyberbezpieczeństwa oraz nad przebudową oferty grantów badawczo-rozwojowych na takie, które będą realnie wspierać rozwój globalnie konkurencyjnych rozwiązań z zakresu cyberbezpieczeństwa nad Wisłą. W ramach działalności grupy *#CyberMadeInPoland* opracowane są i przedstawiane polskiemu rządowi problemy i wyzwania, z jakimi zmaga się branża cyberbezpieczeństwa w Polsce.