Listopad 2017

INSTYTUT KOŚCIUSZKI

BRIEF PROGRAMOWY INSTYTUTU KOŚCIUSZKI

Robert Siudak, Ziemowit Jóźwik

Regionalne centra innowacji w służbie transformacji cyfrowej

autorzy

Robert Siudak – Ekspert Instytutu Kościuszki w dziedzinie innowacji oraz inwestycji w sektorze cyberbezpieczeństwa. Redaktor naczelny kwartalnika European Cybersecurity Market oraz koordynator projektu CYBERSEC HUB. Autor licznych publikacji naukowych w tym dwóch monografii, doktorant w Zakładzie Bezpieczeństwa Narodowego Uniwersytetu Jagiellońskiego. Swoje badania oraz studia prowadził między innymi na Tel-Aviv University oraz Trinity College Dublin.

Ziemowit Jóźwik– Ekspert Instytutu Kościuszki w dziedzinie prawa UE w obszarze cyberbezpieczeństwa. Zastępca redaktora naczelnego European Cybersecurity Market i Koordynator projektów międzynarodowych. Absolwent prawa, ukrainoznawstwa i studiów podyplomowych dla tłumaczy tekstów specjalistycznych z języka ukraińskiego. Koordynował projekty związane z bezpieczeństwem granic i sytuacją na Ukrainie. Współredaktor tomu „Addressing Security Risks at the Ukrainian Border Through Best Practices on Good Governance" (NATO SPS Series).

Regionalne centra innowacji dla cyberbezpieczeństwa

We współpracy z Global EPIC:
Anat Karmona, CyberSpark (Izrael)
David Crozier, Centre for Secure Information Technologies – CSIT (Zjednoczone Królestwo)
Dan Craigen, Global Cybersecurity Resource (Kanada)
Darin Andersen, CyberTECH Network (Stany Zjednoczone)
Richard Franken, The Hague Security Delta (Holandia)

Przodujące centra kompetencji oraz innowacji w dziedzinie cyberbezpieczeństwa tworzone są na całym świecie w formie regionalnych *hubów*. Budowanie lokalnych ekosystemów umożliwia realną oraz wydajną współpracę przedstawicieli uniwersyteckich centrów badań i rozwoju, dużych międzynarodowych firm, lokalnych MŚP oraz startupów. W ramach tak skonstruowanych struktur wypracowywana jest synergia umożliwiająca akumulację oraz przepływ wiedzy, dobrych praktyk i kluczowych kompetencji. Edukacja i szkolenie światowej klasy specjalistów oraz innowatorów zarówno na uczelniach wyższych, jak i poprzez ich udział w pracach sektora prywatnego, umożliwia rozwój średnio i długoterminowych projektów badawczych, a także inwestycje w obiecujące technologie na wczesnym etapie ich rozwoju. W oparciu o tak nakreśloną bazę badań podstawowych oraz stosowanych, rozwijać może się innowacyjny sektor produktów i usług. Poniżej zaprezentowano listę wybranych centrów innowacji dla cyberbezpieczeństwa.

ISSN 1689-9873

CyberSpark (Izrael)

Izrael, ze względu na swoją burzliwą historię, położenie geograficzne oraz niestabilną sytuację polityczną regionu utrzymuje rozbudowaną armię, w tym system jednostek wojska cybernetycznego. Stanowią one kuźnię kadr oraz zaplecze specjalistów dla komercjalnego sektora produktów i usług zabezpieczających infrastrukturę ICT. Wybór inteligentnej specjalizacji w cyberbezpieczeństwie przełożył się na wymierne efekty ekonomiczne dla całej gospodarki. W roku 2015 branża ta wygenerował przychód na poziomie 3,75 miliarda dolarów, co stanowiło ponad 1% PKB[1]. W Izraelu działa aktualnie 365 spółek z sektora cyberbezpieczeństwa, z czego 65 powstało w samym tylko 2016 roku[2]. W tym samym roku izraelskie startupy zajmujące się bezpieczeństwem ICT zebrały 581 mld dolarów finansowania i uplasowały się pod tym kątem na drugim miejscu na świecie, zaraz za amerykańskimi firmami[3].

W roku 2014 przy współpracy Izraelskiego Narodowego Biura Cyberbezpieczeństwa (*Israeli National Cyber Bureau*), administracji rządowej, władz miasta Beer-Sheva, Uniwersytetu Ben Guriona oraz światowych potentatów branży cyber (m.in. Oracle, IBM oraz Lockheed Martin) uruchomiono CyberSpark – izraelską przestrzeń innowacji dla cyberbezpieczeństwa. Wspiera ona zarówno badania jak i rozwój komercyjnych produktów i usług w ramach flagowych inicjatyw:

1) Centrum badań – współtworzone wraz z Uniwersytetem Ber Guriona;
2) Hub B+R – strefa rozwoju komercyjnych projektów wspierana przez ulgi podatkowe oraz publiczne granty;
3) Centrum treningowe – oferujące szkolenia w zakresie cyberbezpieczeństwa;
4) Hub innowacji – platforma networkingowa;
5) Inkubator – wspierający rozwój młodych projektów cyber;
6) Centrum analityczne – skupiono wokół CERT IL.

Administracja państwowa wspiera CyberSpark nie tylko poprzez udostępnianą infrastrukturę, ale także poprzez określone zachęty ekonomiczne: refundację nawet do 30% wynagrodzenia brutto każdego pracownika merytorycznego pracującego nad szczególnie cenioną na rynku technologią czy obniżenie podatku dochodowego przy pracach B+R. Ponadto w ramach budowania regionalnego ekosystemu cyberbezpieczeństwa w Beer Szewie, umiejscowiono narodowy zespół reagowania na incydenty cybernetyczne CERT (*Computer Emergency Response Team*), a także wojskowe jednostki wywiadowcze i technologiczne działające w sektorze cyber.

Centre for Secure Information Technologies (Zjednoczone Królestwo)

Brytyjski sektor produktów i usług bezpieczeństwa ICT stanowi największy narodowy rynek cyberbezpieczeństwa w Unii Europejskiej. W 2015 roku jego szacunkowa wartość wyniosła 4,8 miliarda Euro, odpowiadając 20% całego wspólnotowego rynku[4]. Ponadto

1 Israel's National Cyber Bureau data. (8) HM Government, *The UK Cyber Security Strategy 2011-2016: annual report*, 14.04.2016, https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report [26.10.2017].

2 YL Ventures Ltd, https://techcrunch.com/2017/01/23/trends-in-israels-cybersecurity-investments/ [27.10.2017].

3 Start-Up Nation Central Ltd., www.startupnationcentral.org [27.10.2017].

4 NIS Platform, Business *Cases and Innovation Paths, NIS Platform Working Group 3 (WG3), Final, Version 1.1*; https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents, p. 24–25 [26.10.2017].

3 *(WG3), Final, Version 1.1*, s. 24-25, https://resilience.enisa.europa.eu/nis-platform/shared-documents/wg3-documents [26.10.2017].

Wielka Brytania rozwinęła jeden z najliczniejszych na świecie sektorów cyberbezpieczeństwa zatrudniający aktualnie ponad sto tysięcy osób[5].

Ten komercyjny sukces jest wpierany przez rozbudowaną sieć centrów badawczych dla cyberbezpieczeństwa zrzeszającą 13 ośrodków akademickich w całej Wielkiej Brytanii (*Academic Centres of Excellence in Cyber Security Research*). Tytuł centrum kompetencji nadawany jest uniwersytetom, które prowadzą innowacyjne badania na temat cyberbezpieczeństwa, oraz kształcą światowej klasy specjalistów w tej dziedzinie. Ponadto ważną inicjatywą wspierającą rozwój nowych technologii, w tym w dziedzinie bezpieczeństwa ICT, jest także ogólnonarodowa sieć centrów innowacji, w ramach której zrzeszono 7 ośrodków akademickich (*Innovation and Knowledge Centres*).

Queen's University z Belfastu, znajdujące się zarówno na liście centrów badawczych dla cyberbezpieczeństwa jak i hubów innowacji, utworzyło w roku 2009 Centrum Bezpiecznych Technologii Informatycznych (*Centre for Secure Information Technologies – CSIT*). Jego celem jest stworzenie *hubu* innowacji dla cyberbezpieczeństwa poprzez budowę całościowego ekosystemu interesariuszy lokalnych oraz globalnych. Dlatego też CSIT wspiera aktywnie rozwój klastra cyberbezpieczeństwa w Belfaście (*Belfast Cyber Security Cluster*), który zrzesza ponad 40 firm zatrudniających 1200 pracowników. Ponadto, centrum w ramach swojej działalności przyciągnęło już ponad 100 bezpośrednich inwestycji zagranicznych w sektorze wysokich technologii, a partnerami CSIT są aktualnie takie globalne korporacje jak BAE Systems, Thales Cisco, IBM czy Intel/McAfee. CSIT prowadzi także edukację studentów oraz wewnętrznie prace B+R w obszarach takich jak:

- Bezpieczeństwo infrastruktury krytycznej;
- Uwierzytelnianie urządzeń;
- Wirusy dedykowane na urządzenia mobilne;
- Kryptografia ery post-kwantowej.

5 HM Government, *The UK Cyber Security Strategy 2011-2016: annual report*, 14.04.2016, https://www.gov.uk/government/publications/the-uk-cyber-security-strategy-2011-2016-annual-report [26.10.2017].

The Global Cybersecurity Resource (Kanada)

Kanada stanowi czwarty największy hub innowacji dla cyberbezpieczeństwa na świecie, biorąc pod uwagę wysokość inwestycji Venture Capital w ten sektor w latach 2012-2016 (zaraz po USA, Izraelu oraz Wielkiej Brytanii)[6]. Szczególny ekosystem wykształcił się zwłaszcza w Ontario – stolicy Kanady – gdzie aktywna społeczność ponad 90 startupów oraz MŚP z sektora cyberbezpieczeństwa była w stanie w latach 2011-2015 ściągnąć ponad 250 mln dolarów finansowania od inwestorów VC.

Wykorzystując ten potencjał Uniwersytet Carleton uruchomił w 2016 roku akcelerator biznesowy pod szyldem Globalnego Programu dla Cyberbezpieczeństwa (*The Global Cybersecurity Resource – GCR*). Jest on wspierany z jednej strony przez największy hub innowacji w Ottawie – *Bayview Yards*, z drugiej przez zaplecze akademickie. Pozwala to oprzeć realizację kluczowych biznesowych celów – szybkiego skalowania oraz umiędzynarodowienia oferty młodych spółek – na kompetencjach oraz wiedzy wypracowywanych zarówno na rynku jak i w murach uniwersytetu. Usługi świadczone przez GCR firmom z sektora cyberbezpieczeństwa to m.in.:

- Dostęp do międzynarodowej sieci kontaktów biznesowych poprzez Globalną Platformę Innowacji dla Cyberbezpieczeństwa (*Global EPIC*);

- *Lead to Win Program*, mający za zadanie w okresie trzech lat przeprowadzić spółkę od poziomu idei, przez inkubacje i akceleracje po wzrost oraz ustabilizowanie przychodów na poziomie

6 Deloitte, *Harnessing the cybersecurity opportunity for growth Cybersecurity innovation and the financial services industry in Ontario*, 10.2016, http://www.oce-ontario.org/docs/default-source/default-document-library/oce-tfsa_cyber-brochure-exec-summary-online-oct19.pdf?sfvrsn=4 [26.10.2017].

co najmniej miliona dolarów rocznie. Program ten został uznany za jeden z dziesięciu najlepszych uniwersyteckich inkubatorów w Ameryce Północnej[7].

- Usługi zarządzania bezpieczeństwem – wsparcie oraz dostęp do alertów poprzez kooperacje z centrum operacji cyberbezpieczeństwa (*Security Operations Centre*).

- Dostęp do wyedukowanych kadr, poprzez współpracę z ośrodkami akademickimi kształcącymi cyberspecjalistów przystosowanych do wymagań rynku.

W swoich działaniach GCR kieruje się zasadą „lokalizowania globalnych szans oraz globalizowania lokalnych osiągnięć" (*localize the global and globalize the local*). W związku z tym programy prowadzone przez centrum mają na celu „lokalizowanie" globalnych cybertalentów, technologii oraz funduszy na użytek rozwoju ekosystemu innowacji w Ottawie, a także globalizowanie poprzez eksport oraz promocje lokalnie tworzonych produktów, usług i ekspertyz.

CyberTECH (Stany Zjednoczone)

Pomimo często rozbieżnych szacunków dotyczących wartości globalnego rynku usług i produktów dla cyberbezpieczeństwa, Stany Zjednoczone niezależnie od metodologii badań pozostają ich liderem, z udziałem na poziomie około 20%. Branżową hegemonię USA dobitnie potwierdza lista *Cybersecurity 500* prezentująca pięćset najbardziej innowacyjnych firm z sektora cyber, na której znaleźć można 365 amerykańskich spółek (drugi jest Izrael z 36 firmami)[8].

W oparciu o potencjał Doliny Krzemowej oraz innych ośrodków innowacji w Kalifornii w roku 2013, przy wsparciu administracji stanowej oraz społeczności przedsiębiorców uruchomiono Kalifornijską Grupę Zadaniową ds. Cyberbezpieczeństwa (*California Cybersecurity Task Force)* działającą w formule partnerstwa publiczno-prywatnego. Od roku 2015 na kanwie jej działalności CyberTECH Network uruchomiło projekt *Cyber California*, który ma za zadanie promować ten zachodni stan jako „globalne epicentrum komercyjnego cyberbezpieczeństwa". Szczególny nacisk w ramach współpracy interesariuszy położono na wyzwania technologiczne oraz szanse biznesowe związane z gwałtownym rozwojem Internetu Rzeczy (IoT) oraz wyzwaniem digitalizacji przestrzeni i usług miejskich w ramach koncepcji *Smart & Safe Cities*. W ramach sieci współpracy CyberTECH funkcjonuje szereg inicjatyw podejmowanych zarówno ze strony administracji publicznej jak i podmiotów prywatnych, m.in.:

- Specjalistyczne centra edukacji w dziedzinie cyberbezpieczeństwa tworzone na uniwersytetach oraz collegach stanowych (*Centers of Cybersecurity Excellence in Education*).

- Ekosystem cyberbezpieczeństwa tworzony w ramach *San Diego Cyber Center for Excellence* powołany przy współpracy władz lokalnych, *California State University*, *University of Phoenix* oraz firm zainteresowanych inwestycjami w sektorze cyber w rejonie San Diego (m.in. CyberFlow Analytics, ESET ale także np. Ernst & Young). W ramach hubu funkcjonuje ponad 100 firm zatrudniających 7620 pracowników. Specyfiką regionu jest znaczny udział wojska oraz jego kontraktorów w sektorze cyberbezpieczeństwa (nawet do 50% zatrudnionych).

- Sieć rozwoju przedsiębiorczości *Cybertech Network* oferująca usługi biznesowe oraz wsparcie dla młodych spółek m.in. poprzez przestrzeń coworkingową NEST i sześciomiesięczny program przedsiębiorcy rezydenta oraz działalność Instytutu *Smart & Safe Cities*.

7 Sprott Scholl of Business, *Carleton's Lead To Win program for entrepreneurs named one of top ten in North America*, 4.11.2015, https://sprott.carleton.ca/2015/carletons-lead-to-win-program-for-entrepreneurs-named-one-of-top-ten-in-north-america/ [28.10.2017]

8 Cybersecurity Ventures, *The Cybersecurity 500*, 2017 r. Q1, https://cybersecurityventures.com/cybersecurity-500/ [24.10.2017]

Hague Security Delta (Holandia)

Szacunki dotyczące wartości holenderskiego rynku cyberbezpieczeństwa wahają się w zależności od zastosowanej metodologii od 0,4 do aż 7,5 miliarda euro rocznie[9]. Niezależnie od przyjętych wskaźników, sytuuje to Niderlandy jako jednego z liderów tego sektora w Europie. Administracja publiczna tego kraju prowadzi także szczególnie aktywną politykę zagraniczną na rzecz multilateralnej współpracy w dziedzinie cyberbezpieczeństwa. *Global Commission on the Stability of Cyberspace*, która zainaugurowała swoją działalność w roku 2017, stara się wpierać proces implementacji koherentnych norm w odniesieniu do bezpieczeństwa i stabilności w cyberprzestrzeni. Celem *Global Forum on Cyber Expertise* działającego od 2015 roku, jest natomiast zwiększanie zdolności w cyberprzestrzeni sygnatariuszy porozumienia. Narzędziami wykorzystywanymi w tym celu są nie tylko dobre praktyki i strategie na poziomie politycznym, ale także wybrane standardy techniczne oraz proceduralne. W wypadku obydwóch platform kluczowym państwem inicjującym ich rozwój jest właśnie Holandia.

Najważniejszym klastrem bezpieczeństwa tworzącym w Holandii regionalny ekosystem cyberbezpieczeństwa jest *Hague Security Delta (HSD)*. Zrzesza on aktualnie 239 partnerów, zarówno z sektora prywatnego jak i administracji publicznej. Do jego najważniejszych inicjatyw należą:

- *National Cyber Testbed*[10] – to program budowy narodowej platformy testowania rozwiązań dla cyberbezpieczeństwa w ramach istniejącej infrastruktury publicznej oraz prywatnej. Ma on być w szczególności zogniskowany na rozwiązaniach dla Internetu Rzeczy (ang. *Internet of Things*, IoT) oraz infrastruktury krytycznej. Jego celem jest nie tylko zapewnienie odpowiedniego poziomu bezpieczeństwa, ale także rozwój innowacyjnych produktów i usług w oparciu o testowe wdrożenia możliwe w ramach platformy.

- Punkt *SME Connect* – zapewniający małym i średnim przedsiębiorcom z sektora bezpieczeństwa dostęp do wiedzy na temat możliwości grantowych, partnerstw biznesowych, wyników najnowszych badań, a także animujący dedykowane działania *networkingowe*.

- *Security Startup Accelerator* – uruchomiony we współpracy z *World Startup Factory*, ma na celu wsparcie biznesowe dla rozwoju młodych spółek z obszaru bezpieczeństwa chcących szybko skalować swoją ofertę. W ramach kilkumiesięcznych programów uczestnicy otrzymują m.in. mentoring, dostęp do wiedzy eksperckiej, sieci kontaktów oraz szereg bezpłatnych usług biznesowych.

- *City Deal Urban Security* – program umożliwiający uruchomienie jedenastu ośrodków *living labs* w miastach partnerskich, mający na celu zmierzenie się z miejskimi wyzwaniami bezpieczeństwa przy jednoczesnym dostrzeżeniu w nich szansy rozwojowej dla sektora usług i produktów bezpieczeństwa.

- Kampus HSD – mieści on zarówno Centrum Innowacji, w ramach którego rozwijane są prace B+R oraz inkubacja projektów, jak i Centrum Międzynarodowe, służące wsparciu internacjonalizacji rynku tworzonego w regionie.

HSD było ponadto jednym z głównych organizatorów Cyber Security Week, który miał miejsce w dniach 25–29 września 2017 w Hadze. W jego ramach odbyło się 80 wydarzeń, które zgromadziły 4300 uczestników z 70 krajów, w tym przedstawicieli administracji publicznej, biznesu, akademii oraz trzeciego sektora.

9 André Hendriks, Dick Brandt, Kim Turk (VKA) & Viktoria Kocsis, Daan in 't Veld, Tom Smits (SEO Economisch Onderzoek), 17.05.2016, *Economische Kansen Nederlandse Cybersecurity-Sector: Eenverkenning*. https://www.thehaguesecuritydelta.com/media/com_hsd/report/101/document/economische-kansennederlandse-cybersecurity-sector.pdf [20.10.2016].
Por. The Hague Centre for Strategic Studies, *Dutch investments in ICT and cybersecurity. Putting it in perspective*, Grudzień 2016, https://www.thehaguesecuritydelta.com/media/com_hsd/report/123/document/HCSS-Dutch-Investments-in-ICT.pdf [20.10.2017].

10 The Hague Security Delta, *Verkenning van Nut, Noodzaaken Haalbaarheid van een Nationaal Cybertestbed*, 2016, https://www.thehaguesecuritydelta.com/media/com_hsd/report/115/document/NNH-NCT-DEF-Site.pdf [26.10.2017].

Międzynarodowa współpraca regionalnych ekosystemów cyberbezpieczeństwa

Jak zaprezentowano powyżej, na całym świecie ekosystemy cyberbezpieczeństwa prowadzą działania, które są odpowiedzią na zagrożenia cybernetyczne oraz wspierają możliwości rozwoju gospodarczego. Rozwijają się one w dużej mierze niezależnie, przy wsparciu lokalnych i narodowych aktorów. Liderzy tych kluczowych jednostek dowodzą jednak, że wyzwania związane z cyberbezpieczeństwem wymagają powstania globalnych platform, które zmieniłyby dotychczasowy paradygmat funkcjonowania oraz współpracy, i byłaby odpowiedzią zarówno na globalne jak i lokalne wyzwania. Podstawą tej perspektywy jest wdrożenie międzynarodowej współpracy między regionalnymi ekosystemami w tzw. formule *glocalize,* która polega na wykorzystaniu lokalnie globalnego potencjału, promując jednocześnie najlepsze regionalne rozwiązania na szczeblu międzynarodowym.

Odpowiadając na tak zarysowane potrzeby, 10 października 2017 roku w Krakowie, podczas III Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2017 zainaugurowano działalność platformy o nazwie *Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity* (EPIC). Globalny charakter platformy odzwierciedla jej skład: 13 ekosystemów z 10 krajów świata z 3 różnych kontynentów. Łącząc kompetencje, doświadczenie i fachową wiedzę, ośrodki będą odpowiedzialne za opracowywanie innowacyjnych rozwiązań, umożliwianie wymiany wiedzy, przeprowadzanie analiz i badań, oraz tworzenie standardów na poziomie międzynarodowym. Platforma Global EPIC będzie koncentrowała swoje działania w obrębie 10 priorytetowych obszarów:

1) **Współdzielenie usług biznesowych w obrębie sieci** – Każdy z ekosystemów zobowiązany jest dostarczać zasoby i procesy. Ich skład obejmuje: świadczenie usług z zakresu *softlanding*, umożliwienie łączności z doradcami eksperckimi, wspólne narzędzia i urządzenia operacyjne, informacje specyficzne dla ekosystemu oraz dzielenie się wiedzą i doświadczeniem.
2) **Cyberprojekty** – mają za zadanie umożliwić wdrażanie rozwiązań generowanych przez społeczności dla danego obszaru (np. Internet rzeczy, systemów opieki zdrowotnej i systemów finansowych).
3) **Edukacja przyszłych cybertalentów** – wiąże się z opracowywaniem programów rozwoju w celu podniesienia wiedzy i umiejętności.
4) **Platforma wymiany** – ma umożliwiać tworzenie powiązań między różnymi odmiennymi jednostkami w obrębie ekosystemu, np. łączenie przedsiębiorstwa w jeden ekosystem z konkretnym mentorem w innym ekosystemie.
5) **Ocena zagrożeń** – ma przyczynić się do konstruktywnej dyskusji na temat oceny odporności systemu przed atakami cybernetycznymi.
6) **Cybertreści** – umożliwienie dostępu do treści między organizacjami ekosystemowymi. Przykładami takich treści byłyby zestawy danych, zlokalizowane kanały sieci społecznościowych i artykuły z czasopism.
7) **Odkrywanie zagrożeń –** skanowanie horyzontu, przewidywanie nowy potencjalnych problemów, analiza trendów i badanie teorii nowych domen.
8) **Rzecznictwo** – poprzez globalny zasięg i status platformy, ma ona wspierać oraz zwiększać świadomość, na temat przyczyn, polityk i rekomendacji.
9) **Inwestycje –** mają na celu dążenie do ciągłego ulepszania globalnego programu ramowego w zakresie badań i grają główną rolę przy priorytetyzacji i alokacji budżetu.
10) **Standardy –** zsynchronizowane działania na rzecz ustandaryzowanego rozumienia cyberbezpieczeństwa.

W skład platformy wchodzą aktualnie: CyberSpark (Izrael), Centre for Secure Information Technologies (Zjednoczone Królestwo), The Hague Security Delta (Holandia), Global Cybersecurity Resource – Carleton University (Kanada), University of New Brunswick (Kanada), CyberTech Network (Stany Zjednoczone), Instytut Kościuszki (Polska), Politecnico di Torino (Włochy), La Fundación INCYDE (Hiszpania), CyberWales (Zjednoczone Królestwo), bwtech@UMBC (Stany Zjednoczone), Procomer (Kostaryka), Innovation Boulevard Surrey (Kanada).

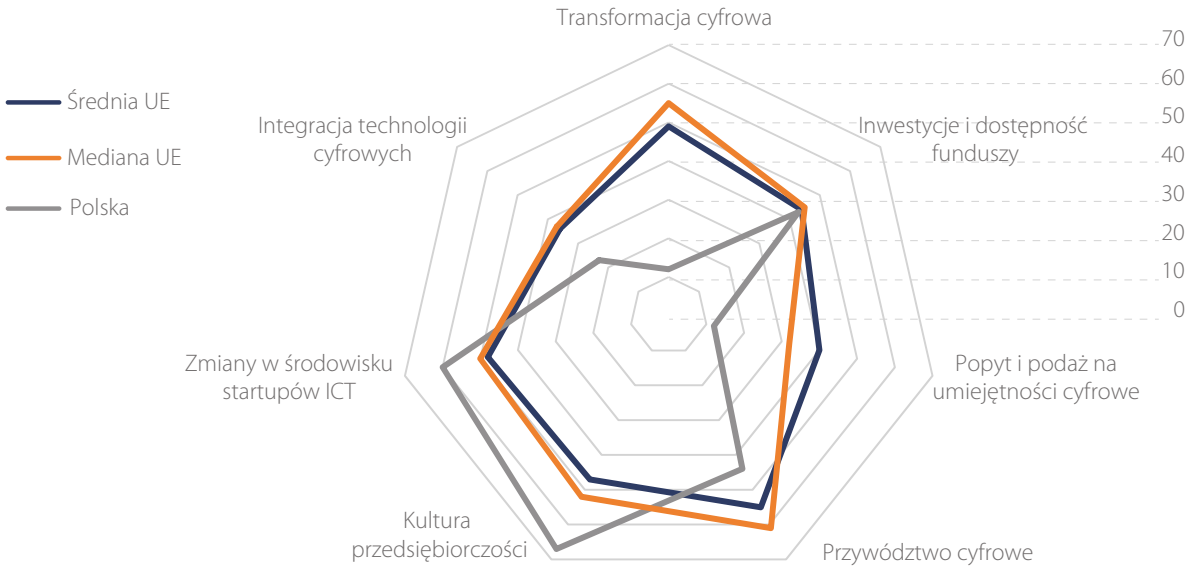
GLOBAL EPIC
Global Ecosystem of Ecosystems Partnership in Innovation and Cybersecurity

Centra Innowacji Cyfrowej w Polsce

Zgodnie z badaniami Komisji Europejskiej (KE) Polska należy do krajów Unii Europejskiej (UE), które dysponują warunkami najmniej sprzyjającymi cyfryzacji gospodarki, pod względem inwestycji, infrastruktury, przywództwa (*e-leadership*), umiejętności oraz kultury przedsiębiorczości. Obok Bułgarii, Chorwacji, Grecji, Łotwy, Rumunii i Węgier, nasz kraj znajduje się wśród państw o najbardziej niedostosowanej do czwartej rewolucji przemysłowej strukturze gospodarki[1]. Chociaż Polska dysponuje istotnym potencjałem w dziedzinie kultury przedsiębiorczości oraz ewolucji ekosystemu startupowego (odpowiednio o 20 pkt. i 12 pkt. przewyższając średnią unijną[2]), odstaje pod względem infrastruktury cyfrowej (np. dostęp przedsiębiorstw do Internetu szerokopasmowego, wykorzystanie systemów CRM i ERP), popytu i podaży na umiejętności cyfrowe (wskaźnik patentów, odsetek zatrudnionych posiadających kompetencje w dziedzinie ICT, wskaźnik zatrudnionych wyposażonych przez pracodawcę w urządzenia mobilne) oraz integracji technologii cyfrowych (wskaźnik przedsiębiorstw, których co najmniej 1% obrotu wytwarzane jest dzięki transakcjom *online*, wielkość obrotu wytwarzana dzięki działalności *e-commerce*, wskaźnik przedsiębiorstw, które realizowały transakcje elektroniczne do innego kraju UE, wykorzystywanie faktur elektronicznych umożliwiających automatyzację procesów księgowych, wykorzystanie w ramach działalności zaawansowanych usług przetwarzania w chmurze, wykorzystanie technologii RFID, wskaźnik przedsiębiorstw korzystających z co najmniej dwu mediów społecznościowych). W ramach powyższych kategorii Polska otrzymała od 13 do 30 punktów poniżej średniej unijnej[3]. W sumie Polska plasuje się na 23 miejscu na 28 państw UE sklasyfikowanych pod względem wsparcia dla transformacji cyfrowej gospodarki.

Podobnie, Polska zajęła 23 miejsce w UE w zestawieniu Komisji Europejskiej *European Innovation Scoreboard 2016*, wyprzedzając jedynie Bułgarię, Chorwację, Rumunię, Łotwę i Litwę, znajdując się w grupie tzw.

Wykres 1. Polska na tle UE Digital Transformation Scoreboard 2017. Źródło: opracowanie własne na podstawie European Commission, *Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses*, January 2017.

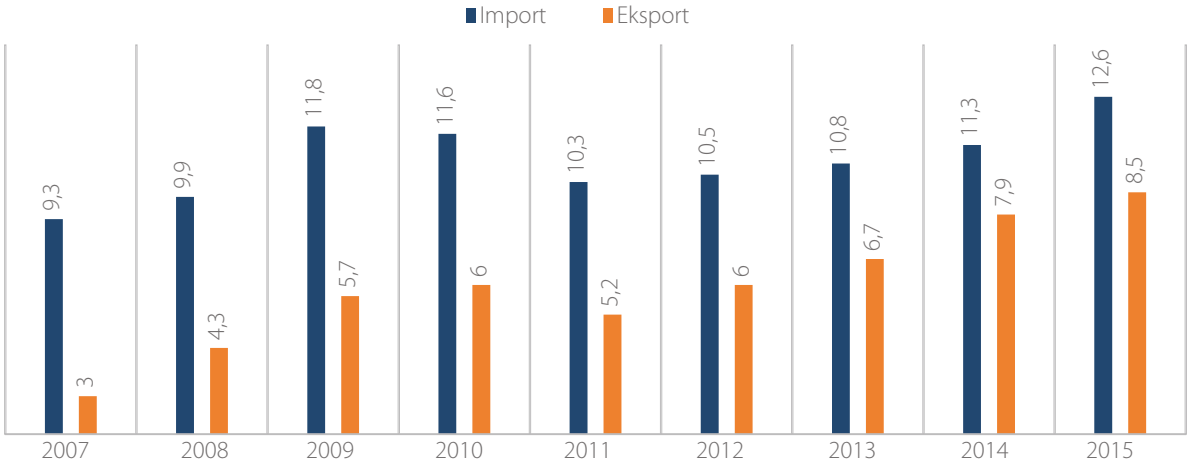


1 European Commission, *Digital Transformation Scoreboard 2017: Evidence of positive outcomes and current opportunities for EU businesses*, January 2017, s. 4, 47.

2 *Ibidem*, s. 103.

3 *Ibidem*, s. 47.

Wykres 2 Udział importu i eksportu produktów wysokiej techniki w imporcie i eksporcie Polski [%].
Źródło: opracowanie własne na podstawie GUS, *Nauka i technika w 2010 r.,* Warszawa 2012. oraz GUS, *Nauka i technika w 2015 r.*, Warszawa 2016.



umiarkowanych innowatorów[4]. Cechą charakterystyczną jest tutaj znikoma rokroczna poprawa wskaźników innowacyjności gospodarki na poziomie 0,1%, który plasuje nasz kraj na 22 miejscu w UE. Jest to szczególnie niekorzystne z uwagi na okoliczność, że niektóre państwa sąsiadujące z nami w rankingu osiągają znacznie wyższe rezultaty (np. Łotwa – 4%, Litwa – 2,4% a Bułgaria – 1,4%)[5]. Wśród wskaźników, które sytuują Polskę znacznie poniżej średniej unijnej warto w kontekście niniejszego opracowania wskazać m.in. niską współpracę pomiędzy innowacyjnymi małymi i średnimi przedsiębiorstwami (MŚP), niewielką ilość przedsiębiorstw, które wdrożyły innowację stworzoną w ramach danego podmiotu oraz ilość innowacji produktowych, procesowych, organizacyjnych i marketingowych w MŚP. Na niskim poziomie pozostają także wydatki na działalność badawczo-rozwojową (B+R) zarówno w sektorze publicznym, jak i prywatnym oraz inwestycje *venture capital*[6]. Tendencję te dobrze oddają dane GUS, zgodnie z którymi nakłady na działalność innowacyjną w 2016 r. zmalały w stosunku do roku poprzedniego w przedsiębiorstwach przemysłowych o 9%, a w przedsiębiorstwach z sektora usług o 15,3%[7].

W zestawieniu *Global Innovation Index*, Polska znalazła się w 2016 r. na 39 miejscu, pozostając w tyle za większością gospodarek unijnych. Warto jednak odnotować, że wynik może odzwierciedlać pozytywną tendencję rozwojową (awans o 7 pozycji w porównaniu do 2015 r.)[8]. Polska gospodarka i eksport w niskim stopniu opierają się na produktach wytwarzanych przez branże wysokiej techniki. Udział wysokiej techniki w eksporcie w 2015 r. utrzymuje się na niskim poziomie – 8,5%. Niezadawalające jest też tempo wzrostu oraz niekorzystne saldo, wskazujące, że Polska pozostaje wciąż importerem nowoczesnych technologii, absorbując dobra wytwarzane za granicą[9].

Zbieżne wnioski dotyczące systemowych niedomagań polskiej gospodarki w obrębie innowacji cyfrowych, można również wysnuć na podstawie śródokresowego przeglądu *Strategii Jednolitego Rynku Cyfrowego*. Jednym z głównych wniosków przedstawionych w dokumencie jest potrzeba ograniczenia dysproporcji pomiędzy najbardziej innowacyjnymi i zaawansowanymi technologicznie regionami UE oraz obszarami, które w niezadawalającym stopniu wykorzystują fundusze UE na rzecz stymulacji

4 European Commission, *European Innovation Scoreboard 2016*, s.12.
5 *Ibidem*, s. 15.
6 *Ibidem*, s. 67 i 86-89.
7 *Działalność innowacyjna przedsiębiorstw w Polsce w latach 2014-2016*, http://stat.gov.pl/obszary-tematyczne/nauka-i-technika-spoleczenstwo-informacyjne/nauka-i-technika/dzialalnosc-innowacyjna-przedsiebiorstw-w-polsce-w-latach-2014-2016,14,4.html [30.10.2017].
8 *The Global Innovation Index 2016. Winning with global innovation*, https://www.globalinnovationindex.org/ [30.10.2017].
9 GUS, *Nauka i technika w 2010 r.*, Warszawa 2012. oraz GUS, *Nauka i technika w 2015 r.*, Warszawa 2016.

innowacyjności i transformacji cyfrowej gospodarki[10]. Podobnie w ewaluacji implementacji *Programu badań, rozwoju technologicznego i innowacji EU Trust and Cybersecurity* finansowanego w ramach grantów z *Siódmego programu ramowego Wspólnoty Europejskiej w zakresie badań, rozwoju technologicznego i demonstracji* (FP7) oraz *Programu Ramowego na rzecz Konkurencyjności i Innowacji* (CIP) na lata 2007-2013 podkreślono niedostateczny udział krajów Europy Środkowo-Wschodniej. Dodatkowo, aktywność podmiotów z naszej części UE okazała się mniejsza niż pierwotnie zakładano[11]. W ramach ewaluacji realizacji celów FP7 podkreślono, że pomimo ogólnego podniesienia poziomu koordynacji działalności B+R w UE, ze względu na niedostateczny udział podmiotów pochodzących z krajów Europy Wschodniej w projektach, ocena ta nie może być w pełni miarodajna[12]. Polska uczestniczyła w sumie tylko w 5 projektach realizowanych w ramach FP7 – dla porównania: Niemcy w 99, Hiszpania w 60, Włochy w 82[13]. Warto jednak mieć na uwadze fakt, że żadne polskie przedsiębiorstwo nie uczestniczyło w projektach badawczo-rozwojowych w ramach FP7, a jeżeli chodzi o udział podmiotów z obszaru Europy Środkowo-Wschodniej – były to jedynie trzy firmy, odpowiednio z Estonii, Węgier oraz Słowenii[14]. Podsumowując dane przedstawione w ewaluacji unijnego dofinansowania działalności badawczo-rozwojowej oraz innowacyjności w dziedzinie cyberbezpieczeństwa w latach 2007-2013, widoczna jest zdecydowana dominacja państw Europy Zachodniej (na całym obszarze Europy Środkowo-Wschodniej zrealizowano ok. 30% projektów, które były implementowane tylko w samych Niemczech)[15]. Zgodnie z analizami Europejskiej Organizacji ds. Cyberbezpieczeństwa (*European Cyber Security Organisation*, ECSO – partner Komisji Europejskiej w realizacji partnerstwa publiczno-prywatnego na rzecz cyberbezpieczeństwa)[16] do głównych barier MŚP w Europie Środkowo-Wschodniej w dostępie do proinnowacyjnych funduszy unijnych zaliczają się m.in. niższe kompetencje językowe oraz słabo skoordynowana i zbiurokratyzowana dystrybucja środków na poziomie instytucji zarządzających. Kolejnym istotnym problemem zdiagnozowanym w ramach prac ECSO był brak kompetencji MŚP z naszego regionu do uczestnictwa w długotrwałych procesach budowania konsorcjów niezbędnych do aplikowania i realizacji projektów wspieranych ze środków UE. Wśród głównych powodów takiego stanu rzeczy należy podkreślić brak odpowiednich funduszy (niechęć lub niemożność inwestycji w działalność B+R). Kolejnym wyzwaniem jest niedostateczna wiedza na temat możliwości oferowanych w ramach unijnych programów wsparcia, a także trudności związane z procesem aplikacyjnym.

Centra Innowacji Cyfrowych

Budowa Centrów Innowacji Cyfrowych jako sieciowych struktur umożliwiających współpracę i kumulację potencjału interesariuszy na rzecz stymulacji działalności badawczo-rozwojowej stanowi szansę na ograniczenie opisywanych powyżej negatywnych zjawisk.

Wspieranie rozwoju Centrów Innowacji Cyfrowych stanowi jeden z kluczowych elementów unijnej strategii Cyfryzacji Europejskiego Przemysłu. Zgodnie z danymi KE, digitalizacja produktów i usług spowoduje, że roczne przychody przemysłu w perspektywie 5 lat w UE wzrosną rocznie o ponad 110 mld euro[17]. Dlatego tak istotne jest, aby rozwijać ośrodki mogące dynamizować ten proces. Europejska sieć Centrów

10 *Jednolity rynek cyfrowy: Komisja wzywa do szybkiego przyjęcia najważniejszych wniosków ustawodawczych oraz określa przyszłe wyzwania*, http://europa.eu/rapid/press-release_IP-17-1232_pl.htm [20.06.2017]

11 Commission Staff Working Document, *An assessment of the implementation and participation in the EU Trust and Cybersecurity RTD and innovation programme funded by FP7 and CIP grants (2007 – 2013)*. Accompanying the document – *Commission Decision on the signing of a contractual arrangement on a public-private partnership for cybersecurity industrial research and innovation between the European Union, represented by the Commission, and the stakeholder organisation*, C(2016) 4400 final, SWD(2016) 215 final, SWD(2016) 216 final, SWD(2016) 210 final, 2016, s. 29.

12 *Ibidem*, s. 26.

13 *Ibidem*, s. 33.

14 *Ibidem*, s. 32.

15 W sumie 32 – w porównaniu do 99 w Niemczech (Bułgaria – 3, Czechy – 7, Estonia – 5, Węgry – 4, Polska – 5, Rumunia – 8, Słowenia – 2).

16 Position Paper WG4, *Support to SME's, coordination with countries (in particular East EU) and regions. Draft document with initial description of priorities and activities*, s. 6.

17 European Commission, *Digital Single Market – Digitising European Industry Questions & Answers*, Bruksela, 10.04.2016, http://Europa.Eu/Rapid/Press-Release_MEMO-16-1409_En.Htm [30.10.2017].

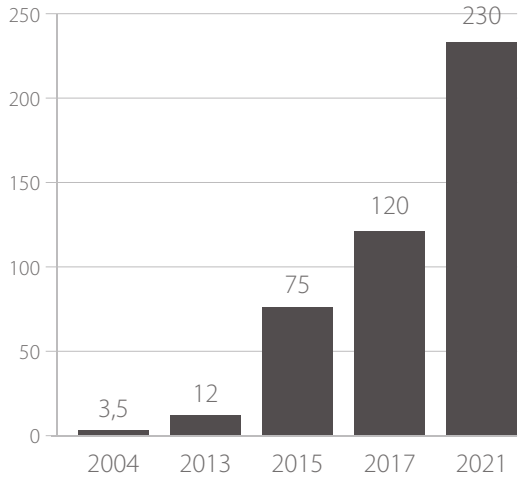
Innowacji Cyfrowych (*Digital Innovation Hubs*), nakierowanych na dostarczanie europejskiemu przemysłowi zaawansowanych kompetencji i technologii cyfrowych ma być siłą napędową gospodarki 4.0 w Europie[18]. Główne działania UE na rzecz rozwoju Centrów Innowacji Cyfrowych to:

- mobilizacja funduszy regionalnych oraz strukturalnych w celu budowania regionalnych i krajowych struktur będących centrami referencyjnymi w ramach tworzenia innowacji cyfrowych w wybranych regionach UE;
- przeznaczenie 500 mln euro na budowanie Europejskiej sieci Centrów Innowacji Cyfrowych w ramach Programu *Horyzont 2020*, w celu współpracy innowacyjnych ekosystemów w kontekście głównych wyzwań rozwojowych;
- mobilizacja środków Komisji Europejskiej na rzecz budowania międzynarodowych sieci, integracja rozproszonych działań w jeden system wsparcia dla międzyregionalnych innowacyjnych ekosystemów, wydzielenia specjalnych środków w ramowych programów finansowania oraz budowanie Centrów Innowacji Cyfrowych w mniej rozwiniętych regionów UE.

Dodatkowo KE planuje wspierać rozwój Centrów Innowacji Cyfrowych w państwach, które dołączyły do UE po 2004 roku[19]. Ma to pozwolić na niwelowanie dysproporcji rozwojowych pomiędzy poszczególnymi regionami oraz stanowi odpowiedź na zdiagnozowane problemy z działalnością innowacyjną i cyfryzacją gospodarki. Wpisując się zatem w główne kierunki polityki proinnowacyjnej UE, Polska mogłaby zostać regionalnym liderem w tym obszarze i agregować innowacyjny potencjał Europy Środkowo-Wschodniej poprzez tworzenie sprzyjających warunków do prowadzenia działalności gospodarczej z obszaru nowych technologii dla przedsiębiorstw z regionu tzw. Trójmorza.

Z uwagi na dynamiczny rozwój światowego rynku cyberbezpieczeństwa, który to sektor w 2021 r. ma osiągnąć wartość 230 mld USD, rosnące zainteresowanie UE rozwijaniem zasobów przemysłowych i technologicznych w tym obszarze oraz zbieżność z interesami bezpieczeństwa krajowego oraz możliwych impulsów pobudzających innowacyjność gospodarki, cyberbezpieczeństwo stanowi jeden z najciekawszych obszarów, który może być rozwijany w ramach Centrów Innowacji Cyfrowych[20].

Wykres 3 Wartość światowego rynku cyberbezpie-czeństwa (w mld USD).
Źródło: Siudak R., *Nowoczesny i Innowacyjny Sektor ICT: Kluczowa Część Krajowego Ekosystemu Cyberbezpieczeństwa* [w:] *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*, Instytut Kościuszki, 2017.



Wzmacnianie krajowych kompetencji oraz zasobów technologicznych w obszarze cyberbezpieczeństwa na świecie realizowana jest poprzez centra innowacji

18 European Commission, *Digitalising European Industry*, https://ec.europa.eu/digital-single-market/en/policies/digitising-european-industry [30.10.2017].

19 European Commission, *Call for Digital Innovation Hubs in EU13 Member States*, https://ec.europa.eu/digital-single-market/en/news/call-digital-innovation-hubs-eu13-member-states [30.10.2017].

20 Siudak R., *Nowoczesny i Innowacyjny Sektor ICT: Kluczowa Część Krajowego Ekosystemu Cyberbezpieczeństwa* [w:] *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*, Instytut Kościuszki, 2017, s. 48. Opracowanie własne na podstawie: Gartner, *Forecast Analysis: Information Security, Worldwide*, 1Q16 Update, 2016; Visiongain, *Cyber Security Market Report 2016-2021, 2016; Cybersecurity Ventures, Cybersecurity Market Report Q1 2017, 2017; Markets and Markets, Cyber Security Market by Solutions (IAM, Encryption, DLP, UTM, Antivirus/Antimalware, Firewall, IDS/IPS, Disaster Recovery), Services, Security Type, Deployment Mode, Organization Size, Vertical & Region – Global Forecast to 2021, 2016.*

rozwijające się w ramach regionalnych ekosystemów, które umożliwiają współpracę przedstawicieli uniwersyteckich centrów B+R, lokalnych MŚP oraz startupów, a także dużych firm (zarówno międzynarodowych korporacji, jak i liderów krajowych). W ramach takich sieciowych struktur wypracowywana jest synergia umożliwiająca akumulację oraz przepływ wiedzy, dobrych praktyk i kluczowych kompetencji. Poniżej zostaną przedstawione ramowe rekomendacje dotyczące budowania tego typu platform współpracy zebrane w ramach III Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC 2017.

Ekosystemy regionalne

W kontekście rozbudowy zasobów technologicznych i przemysłowych w obszarze cyberbezpieczeństwa w ramach Centrów Innowacji Cyfrowych szczególnego podkreślenia wymaga rola regionów w procesie stymulowania innowacyjnej gospodarki. To właśnie w regionach skoncentrowany jest główny „strategiczny zasób" – wiedza wynikająca z bezpośrednich interakcji w ramach ekosystemu, w skład którego wchodzi kultura organizacyjna, infrastruktura, umiejętna polityka proinnowacyjna lokalnej administracji publicznej oraz potencjał badawczo-rozwojowy ośrodków naukowych[21]. Również Najwyższa Izba Kontroli w Raporcie „Wdrażanie innowacji przez szkoły wyższe i parki technologiczne" stwierdziła, że część z parków technologicznych nie była w stanie efektywnie realizować swych zadań polegających na tworzeniu warunków do rozwoju firm technologicznych i innowacyjnych, a także zapewnianie warunków do rozwoju innowacyjnych przedsięwzięć i udzielaniu pomocy nowopowstałym firmom w początkowej fazie ich funkcjonowania, z uwagi na położenie w regionach o niewystarczającym potencjale innowacyjnym i słabszym rozwoju[22]. Dlatego największe szanse na powodzenie we wspieraniu rozwoju innowacyjnych rozwiązań w wyspecjalizowanych obszarach technologicznych, jak np. cyberbezpieczeństwo, mają podmioty, które są w stanie wykorzystać istniejący w danym regionie „strategiczny zasób". Relację pomiędzy uwarunkowaniami regionalnymi a sukcesem Centrów Innowacji Cyfrowych w obszarze cyberbezpieczeństwa dobrze oddają zaprezentowane w niniejszym opracowaniu przykłady, gdzie istnieją specyficzne powiązania pomiędzy lokalnymi wiodącymi ośrodkami akademickimi, sektorem prywatnym i administracją publiczną (np. izraelski CyberSpark). Godne odnotowania jest dostrzeżenie tej okoliczności w *Strategii na rzecz Odpowiedzialnego Rozwoju oraz Krajowych Ramach Polityki Cyberbezpieczeństwa RP 2017-22* w przedmiocie Cyberpark Enigma na bazie wiodących ośrodków naukowo-badawczych (Warszawa, Kraków, Wrocław, Poznań i Trójmiasto) oraz stworzenie Naukowego Klastra Cyberbezpieczeństwa.

Centrum badawczo-rozwojowe oraz rozbudowa oferty edukacyjnej i szkoleniowej

Biorąc pod uwagę stale zwiększającą się lukę zatrudnienia w obszarze cyberbezpieczeństwa oraz potrzebę tworzenia innowacyjnych rozwiązań, które będą nadążać za dynamicznym rozwojem zagrożeń, konieczne jest aby Centrum Innowacji Cyfrowych stanowiło również centrum kompetencji w obszarze cyberbezpieczeństwa. Centrum Innowacji Cyfrowych powinno ściśle współpracować z wiodącymi ośrodkami akademickimi. Pozwala to na poszerzenie oferty edukacyjnej, a także ułatwienie działalności badawczo-rozwojowej oraz późniejsze wdrożenie i komercjalizację efektów tych prac. Centrum Innowacji Cyfrowych umożliwia stałą wymianę wiedzy i doświadczeń pomiędzy światem nauki oraz przedsiębiorstwami. Zapewnia to sektorowi prywatnemu trwały dostęp do innowacji i efektów działalności badawczo-rozwojowej, natomiast środowisku naukowemu możliwość wdrożenia i praktycznego wykorzystania swoich rozwiązań, dostęp do wiedzy z zakresu prowadzenia działalności gospodarczej, funkcjonowania rynku, a także możliwość uzupełnienia kadry naukowej o specjalistów zatrudnionych w firmach. Przykładem tego typu formuły jest współpraca CyberSpark z Uniwersytetem Ber Guriona w Beer Szewie lub kandyjskiego Global Cybersecurity Resource z Uniwersytetem Carleton. Omówiony poniżej krakowski CYBERSEC HUB współpracuje zarówno z Politechniką Krakowska, jak i Akademią Górniczo-Hutniczą, będąc jednym z partnerów tworzonego na tej uczelni Centrum Cyberbezpieczeństwa.

21 Gust-Bardon N., *Innowacyjność w aspekcie regionalnym*, https://www.ur.edu.pl/file/15836/05.pdf [30.10.2017].

22 Najwyższa Izba Kontroli, *Wdrażanie innowacji przez szkoły wyższe i parki technologiczne*, Warszawa 2013.

Platforma wymiany informacji

Jednym z ważnych elementów Centrum Innowacji Cyfrowych, szczególnie w krajach Europy Środkowo-Wschodniej jest budowa platformy wymiany informacji umożliwiającej pozyskiwanie aktualnych wiadomości o formach publicznego wsparcia dla przedsiębiorstw, inwestycjach, potencjalnych partnerach biznesowych. Tego rodzaju platforma ułatwiałaby mapowanie interesariuszy sektora cyberbezpieczeństwa, budowanie konsorcjów, aplikowanie o środki publiczne, realizację wspólnych projektów, przedsięwzięć i działań marketingowych oraz dostęp do analiz rynkowych oraz diagnoz zapotrzebowania na dane rozwiązania. Również ze wspomnianych już wyżej prac ECSO wynika, że krokiem, który mógłby przynieść natychmiastowe efekty w postaci zwiększenia udziału podmiotów z Europy Środkowo-Wschodniej w unijnych proinnowacyjnych programach wsparcia w obszarze cyberbezpieczeństwa, byłoby utworzenie platformy wymiany informacji w dziedzinie bieżących zagrożeń cybernetycznych oraz funduszu bezpośredniego umożliwiającego realizację projektów na rzecz zwiększenia odporności cybernetycznej MŚP[23] lub specjalnych, łatwych do pozyskania małych grantów na budowę podstawowej infrastruktury zapewniającej cyberbezpieczeństwo MŚP[24].Proponowane środki zaradcze w tym obszarze zakładają także sporządzenie dopasowanego do warunków regionalnych zbioru dobrych praktyk na podstawie doświadczeń przedsiębiorstw zachodnioeuropejskich w przedmiocie realizacji projektów unijnych[25]. Pomóc w rozpowszechnianiu informacji na temat form wsparcia UE mogłoby też wykorzystanie mediów społecznościowych, platform cyfrowych oraz platform ułatwiających nawiązywanie kontaktów biznesowych[26]. Centra Innowacji Cyfrowych powinny upowszechniać wiedzę na temat możliwości unijnego wsparcia dla działalności B+R lokalnych MŚP, pomagać w budowaniu konsorcjów i aplikowaniu o środki UE, gwarantując stabilne zaplecze finansowe, infrastrukturalne oraz eksperymentalne do testowania wdrożeń oraz pośredniczyć w kontaktach z instytucjami zarządzającymi i administracją publiczną (lokalną, krajową i unijną). Jest to szczególnie istotne dla przedsiębiorstw z naszego regionu, które nie posiadają odpowiednich zasobów i kompetencji, aby na bieżąco monitorować i brać udział w procesie decyzyjnym na poziomie UE (w przeciwieństwie do przedsiębiorstw z Europy Zachodniej, które mają wypracowane strategie *government affairs*, prowadzenia działalności lobbingowej i budowania relacji z najważniejszymi unijnymi interesariuszami sektora cyberbezpieczeństwa).

Inkubator oraz akcelerator innowacyjnych startupów

Z uwagi na bezprecedensową dynamikę ewolucji zagrożeń cybernetycznych, rozwiązania bezpieczeństwa teleinformatycznego, muszą być ciągle aktualizowane i rozwijane. Skuteczna ochrona przed zagrożeniami płynącymi z cyberprzestrzeni wymaga „radykalnej innowacyjności"[27]. Zjawisko to premiuje innowacyjną, często niszową ofertę startupów, która jest w stanie nadążyć za dynamicznie zmieniającym się krajobrazem zagrożeń w kontekście m.in. Internetu rzeczy (*IoT*), bezpieczeństwa bezzałogowych statków powietrznych, cyberubezpieczeń, zarządzania podatnościami i ryzykiem[28] a także technologii *blockchain* czy sztucznej inteligencji. O roli startupów na rynku cyberbezpieczeństwa świadczy, że na liście *500 Cybersecurity* w 2017 r. w pierwszej dziesiątce oprócz globalnych liderów technologicznych znalazły się aż trzy startupy. Dodatkowo warto uwzględnić okoliczność, że część pozostałych firm w czołówce zawdzięcza sukces przejęciom innowacyjnych rozwiązań startupów. Model rozwoju oparty na działaniu w warunkach wysokiego ryzyka oraz w celu znacznej i szybkiej skalowalności oferty, z jednej strony pomaga osiągnąć omawianą powyżej dużą dynamikę wzrostu całego sektora, z drugiej – wymaga jednak systemowego wsparcia startupów.

23 Position Paper WG4, *Support to SME's, coordination with countries (in particular East EU) and regions. Draft document with initial description of priorities and activities*, s. 7.

24 Position Paper WG4, *Support SME, coordination with countries (in particular East EU) and regions. Preparatory notes*, s.5.

25 Position Paper WG4, *Support to SME's, coordination with countries (in particular East EU) and regions. Draft document with initial description of priorities and activities*, s. 7.

26 Position Paper WG4, *Support SME, coordination with countries (in particular East EU) and regions. Preparatory notes.*, s.5.

27 Tabansky L., *Rozwój innowacyjności. Studium przypadków współpracy publiczno-prywatnej w wybranych państwach* [w:] *Bezpieczeństwo poprzez innowacje. Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego*, Instytut Kościuszki, Kraków 2017, s. 29-44.

28 Leitersdorf Y., Schreiber O., Reznikov I., *Trends in Israel's cybersecurity investments*, Crunch Network, 23/012017, https://techcrunch.com/2017/01/23/trends-in-israels-cybersecurity-investments/ [30.10.2017].

W tym celu Centrum Innowacji Cyfrowych powinno uruchamiać programy inkubacyjne i akceleracyjne w celu ułatwienia rozwoju innowacyjnych rozwiązań startupów w kluczowym i często najtrudniejszym dla nich wczesnym okresie rozwoju (tzw. faza *seed* lub *pre-seed*). W ramach programu akceleracyjnego Centrum Innowacji Cyfrowych powinno oferować:

- wsparcie finansowe działalności;
- wsparcie infrastrukturalne (zaplecze biurowe, wsparcie w obsłudze biurokratycznej, wsparcie promocyjne i marketingowe);
- program szkoleń z zakresu rozwoju produktów, sprzedaży, skalowania działalności, UX (*user experience*), tworzenia strategii eksportowej i internacjonalizacji działalności;
- możliwość współpracy z mentorami – ekspertami w dziedzinie prowadzenia działalności gospodarczej dysponującymi wiedzą na temat funkcjonowania danego sektora rynku i możliwości wsparcia dla przedsiębiorstw oraz kontaktami biznesowymi,
- dostęp do sieci kontaktów, potencjalnych partnerów biznesowych z sektora prywatnego, jak i publicznego (stanowiących partnerów akceleratora), a także inwestorów operujących w ramach danego sektora rynku;
- możliwość zaprezentowania swojego rozwiązania podczas wydarzenia podsumowującego daną edycję programu akceleracyjnego (tzw. *demo day*)

Tworzenie programów akceleracyjnych, udzielanie wsparcia dla startupów z obszaru cyberbezpieczeństwa stanowi kluczowy element, fundament Centrum Informacji Cyfrowych. Pokazuje to dobitnie przykład kanadyjskiego Global Cybersecurity Resource, którego początki sięgają właśnie uruchomienia akceleratora na Uniwersytecie Carleton. Biorąc pod uwagę charakterystykę rynku cyberbezpieczeństwa (dynamika ewolucji krajobrazu zagrożeń, model rozwoju oparty na działaniu w warunkach wysokiego ryzyka, postęp technologiczny), niezbędne jest, aby rozwijać różnorodne formy eksperckiego wsparcia dla przedsiębiorstw.

Budowanie relacji z dużymi przedsiębiorstwami

Istotnym czynnikiem budującym sukces Centrów Innowacji Cyfrowych jest umiejętne budowanie relacji z sektorem prywatnym – krajowymi liderami branży ICT, globalnymi korporacjami oraz spółkami skarbu państwa. Z jednej strony mogą one stać się beneficjentami technologii wytwarzanych w ramach Centrum Innowacji Cyfrowych (na zasadzie *one-stop-shop*), stać się jego partnerami biznesowymi lub inwestorami czy rozbudowywać swoje kompetencje poprzez współpracę z zaangażowanymi podmiotami akademickimi. Z drugiej strony natomiast są w stanie zaoferować startupom unikalne warunki testowania wdrożeń innowacyjnych rozwiązań (na wzór programu *National Cyber Testbed* holenderskiego *Hague Security Delta*), rozwijanie kompetencji biznesowych czy szanse nawiązanie licznych kontaktów międzynarodowych. Udział dużych przedsiębiorstw o ustabilizowanej pozycji rynkowej i renomie, pomógłby również w budowaniu zaufania do młodych, innowacyjnych spółek, dla których barierą rozwojową jest brak odpowiedniego dorobku, który jest szczególnie istotny w tak wrażliwym sektorze jak cyberbezpieczeństwo.

Współpraca międzynarodowa

Z uwagi na charakterystykę zagrożeń cybernetycznych oraz współzależności, eksterytorialności i intensyfikacji transgranicznych kontaktów biznesowych w ramach współczesnej gospodarki cyfrowej, Centra Innowacji Cyfrowych muszą rozwijać współpracę międzynarodową. Podobnie jak komunikują się organy rządowe – np. w ramach Grupy Współpracy NIS, czy też mechanizmu CBM (środki budowy zaufania, z ang. *Confidence Building Measures*) w ramach Centrum Zapobiegania Konfliktom OBWE, *Global Commission on the Stability of Cyberspace* lub *Global Forum on Cyber Expertise*, ośrodki wsparcia innowacji w obszarze cyberbezpieczeństwa powinny pozostawać w kontakcie, współpracować, wymieniać się informacjami. Taką rolę pełni Globalna Platforma Innowacji dla Cyberbezpieczeństwa (*Global EPIC – Global Ecosystem of Ecosystems Platform in Innovation and Cybersecurity*) zrzeszająca 14 podmiotów z 10 państw. Celem porozumienia jest rozwijanie współpracy

międzynarodowej regionalnych ekosystemów w tzw. formule *glocalize* polegającej na wykorzystaniu w wymiarze lokalnym globalnego potencjału przy jednoczesnym promowaniu najlepszych lokalnych rozwiązań na całym świecie. Global EPIC skupia się wokół 10 priorytetowych obszarów, m.in. wsparcie inwestycji, współdzielenie usług biznesowych oraz zasobów eksperckich, edukacja czy analiza rynków pod kątem nowych trendów.

Zaangażowanie administracji publicznej

Administracja publiczna, jako lider krajowego systemu cyberbezpieczeństwa, powinna być jednym z uczestników Centrum Innowacji Cyfrowych. Mowa tu zarówno o organach samorządu terytorialnego i administracji lokalnej (w ramach danego ekosystemu regionalnego), ale także władzy centralnej. Jak pokazuje doświadczenie światowych liderów cyberbezpieczeństwa (Wielka Brytania, Izrael), sektor ten nie może rozwinąć się bez aktywnego zaangażowania państwa zarówno w domenie cywilnej, jak i wojskowej. Od realizacji strategii cyberbezpieczeństwa, poprzez stworzenie odpowiednich mechanizmów współpracy, do programu badań i rozwoju – państwo powinno wspierać rozwój sektora cyberbezpieczeństwa. Dlatego Centrum Innowacji Cyfrowych powinno angażować przedstawicieli administracji publicznej na wielu płaszczyznach działalności. W przypadku izraelskiego Cyber Spark, państwo wspiera nie tylko poprzez udostępnianą infrastrukturę ale także za pomocą zachęt ekonomicznych i fiskalnych. W Wielkiej Brytanii, Centrala Łączności Rządowej (*GCHQ*) współtworzy akcelerator innowacyjnych startupów[29] oraz program edukacyjny *Cyber First*. Administracja publiczna może być również beneficjentem rozwoju Centrum Innowacji Cyfrowych – zarówno w kontekście pozyskiwania technologii zwiększających bezpieczeństwo teleinformatyczne danej jednostki organizacyjnej (np. urzędu), jak i długoterminowej realizacji celów proinnowacyjnej polityki państwa.

Wsparcie Centrów Innowacji Cyfrowych wpisuje się zarówno w *Strategię na rzecz Odpowiedzialnego Rozwoju* – w kontekście realizacji programu rozwojowego Cyberpark Enigma, jak i *Krajowe Ramy Polityki Cyberbezpieczeństwa RP 2017-22*, których jednym z celów szczegółowych jest rozbudowa krajowych zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa.

Polskie doświadczenie – CYBERSEC HUB

Animowany przez Instytut Kościuszki CYBERSEC HUB stanowi pierwszą w Polsce próbę uruchomienia centrum kompetencji i innowacji w obszarze cyberbezpieczeństwa. Wykorzystując unikalny potencjał Krakowa (środowisko akademickie, wysokie kompetencje IT, lokowanie centrów bezpieczeństwa międzynarodowych korporacji, prężny ekosystem startupowy) od 2016 r. w ramach sieciowej struktury, w skład której wchodzą przedstawiciele lokalnej administracji publicznej, uczelni, instytucji otoczenia biznesu, środowiska eksperckiego i firm technologicznych, wspierany jest rozwój MŚP oraz startupów tworzących rozwiązania w obszarze cyberbezpieczeństwa. CYBERSEC HUB skupia swoje działania wokół 8 priorytetowych obszarów:

1) Wprowadzenie problematyki cyberbezpieczeństwa do programu studiów na uczelniach wyższych (Akademia Górniczo-Hutnicza, Politechnika Krakowska, Uniwersytet Jagielloński);

2) Stymulowanie rozwoju innowacyjnych produktów i usług dla cyberbezpieczeństwa m.in. w formule *real living labs*;

3) Pomoc w internacjonalizacji działalności startupów oraz MŚP oferujących produkty oraz usługi w dziedzinie cyberbezpieczeństwa;

4) Wzmocnienie współpracy badawczej oraz dydaktycznej pomiędzy przedstawicielami biznesu i uniwersytetami z regionu;

5) Wspieranie rozwoju rynku wewnętrznego poprzez łączenie odbiorców oraz producentów produktów i usług dla cyberbezpieczeństwa w regionie;

29 Forbes, *First Cybersecurity Startups Graduate from the UK Intelligence's GCHQ Accelerator*, 25 April 2017, https://www.forbes.com/sites/montymunford/2017/04/25/first-cybersecurity-startups-graduate-from-the-uk-intelligences-gchq-accelerator/#74fd8c5963de [30.10.2017].

6) Stworzenie w ramach *hubu* punktu agregującego wiedzę na temat rynku cyberbezpieczeństwa działającego w formule *one-stop-shop*;

7) Ściągnięcie do regionu inwestycji międzynarodowych z sektora cyberbezpieczeństwa;

8) Stworzenie Centrum Wysokich Kompetencji w dziedzinie cyberbezpieczeństwa z ośrodkiem badań interdyscyplinarnych nad cyberbezpieczeństwem.

W ramach CYBERSEC HUB zrealizowano m.in.:

- Program CYBERSEC ACCELERATOR wspierający internacjonalizację działalności 7 innowacyjnych startupów i MŚP z Małopolski poprzez udział w misjach gospodarczych do USA, Izraela i Wielkiej Brytanii, promocję podczas II Polskiego Forum Cyberbezpieczeństwa oraz II i III Europejskiego Forum Cyberbezpieczeństwa (specjalna strefa CYBERSEC HUB expo), mentoring ekspercki w obszarze strategii eksportowej oraz ułatwianie kontaktów z inwestorami;

- Organizacja *Ścieżki Przyszłość* podczas II i III Europejskiego Forum Cyberbezpieczeństwa poświęconych rozwojowi innowacji oraz inwestycji, współpracy międzynarodowej i promocji technologii tworzonych przez startupy;

- Liczne wydarzenia branżowe ułatwiające nawiązywanie kontaktów biznesowych – m.in. konferencje i spotkania wyjazdowe z partnerami lokalnymi (m.in. *European Enterprise Network*, organizacje środowiska startupowego), specjalny *Cybersecurity Evening* w Ambasadzie RP w Londynie nakierowany na promocję polskich rozwiązań w Wielkiej Brytanii, udział w ministerialnej misji gospodarczej do USA);

- Wizyty studyjne inwestorów zagranicznych i krajowych w instytucjach lokalnego ekosystemu startupowego;

- Publikacje kwartalnika *European Cybersecurity Market* poświęconego ewolucji europejskiego rynku cyberbezpieczeństwa i ekosystemu startupowego oraz innowacyjnym technologiom oraz katalogu *CYBERSEC HUB Innovation Book* promującego lokalne rozwiązania lokalnych startupów i MŚP;

- Utworzenie Centrum Cyberbezpieczeństwa Akademii Górniczo-Hutniczej oraz dyskusje na temat rozszerzenia oferty edukacyjnej krakowskich uczelni w obszarze cyberbezpieczeństwa;

- Inaugurację dzielności platformy Global EPIC, której CYBERSEC HUB (Instytut Kościuszki) jest jednym z członków-założycieli;

- Szereg spotkań z przedstawicielami administracji lokalnej oraz centralnej, jak i wiodących firm technologicznych na temat rozwoju regionalnej specjalizacji w obszarze cyberbezpieczeństwa.

Zadanie publiczne współfinansowane przez Ministerstwo Spraw Zagranicznych RP w ramach konkursu Dyplomacja publiczna 2017 – komponent „Wymiar samorządowy i obywatelski polskiej polityki zagranicznej 2017". Publikacja wyraża jedynie poglądy autora i nie może być utożsamiana z oficjalnym stanowiskiem Ministerstwa Spraw Zagranicznych RP.

Rzeczpospolita Polska
Ministerstwo
Spraw Zagranicznych

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 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

Dalsze informacje i komentarze: Magdalena Bujak, magdalena.bujak@ik.org.pl, tel. +48 12 200 23 69