Bezpieczeństwo poprzez innowacje

Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego

Wiesław Goździewicz, Cyprian Gutkowski,
Lior Tabansky, Robert Siudak
Editor: Dominik Skokowski

Instytut Kościuszki

BEZPIECZEŃSTWO POPRZEZ INNOWACJE

SEKTOR CYBERBEZPIECZEŃSTWA JAKO SIŁA NAPĘDOWA WZROSTU GOSPODARCZEGO

Wiesław Goździewicz, Cyprian Gutkowski,
Lior Tabansky, Robert Siudak

Redakcja: Dominik Skokowski

INSTYTUT KOŚCIUSZKI

Nie wszystkie opinie wyrażone w niniejszej publikacji przez jej autorów odzwierciedlają oficjalne stanowisko programowe Instytutu Kościuszki oraz partnerów publikacji. Stanowią one wkład w debatę publiczną. Tezy zawarte w publikacji odzwierciedlają stanowiska poszczególnych autorów, niekoniecznie stanowiąc opinie pozostałych.

Bezpieczeństwo poprzez innowacje
Sektor cyberbezpieczeństwa jako siła napędowa wzrostu gospodarczego

Autorzy: Wiesław Goździewicz, Cyprian Gutkowski, Lior Tabansky, Robert Siudak

Redakcja: Dominik Skokowski

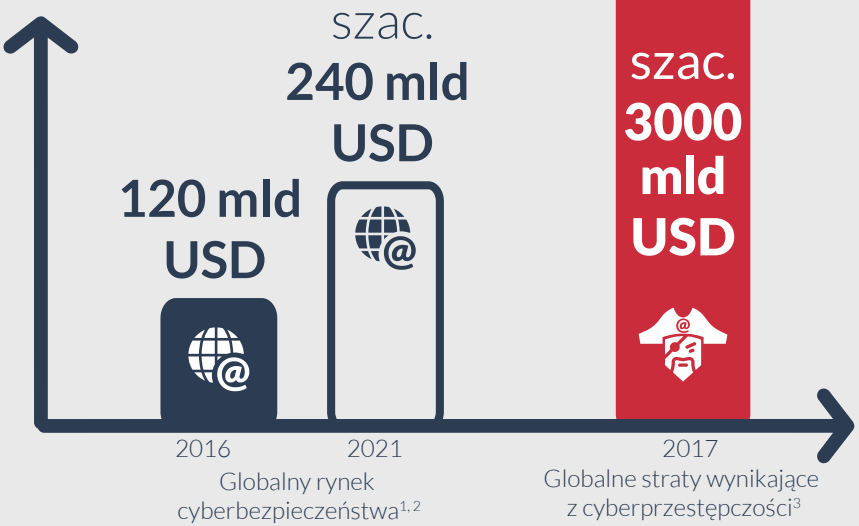
Ikony z the Noun Project: European Union, Nato, Poland, Israel, Pirate by anbileru adaleru, Partnership, Internet, Organization, Product Research by Gregor Cresnar, Euro by Estelle Philibert, Mortar Board by PJ Souders, Programmer By Kid A, Successful Programmer by Gan Khoon Lay, Poland by Hea Poh Li Union Jack by Christian, Shield by Kimmi Studio, Partnership by Delwar Hossain, Handshake by Becris, Black Hat Hacker by Luis Prado, Global User by icon 54, Teamwork by Becris, arrow by Vladimir Belochkin, Shield by Creative Stall, PK.

Instytut Kościuszki
ul. Feldmana 4/9-10
31-130 Kraków
e-mail: ik@ik.org.pl
+48 12 632 97 24
www.ik.org.pl
ISBN 978-83-63712-30-3

SPIS TREŚCI

PODSUMOWANIE

Cyberbezpieczeństwo to nie tylko koszty. Odpowiednio zaprojektowany krajowy sektor cyberbezpieczeństwa pozwala zarówno zwiększyć bezpieczeństwo krajowych instytucji i przedsiębiorstw, jak i generować znaczące wpływy budżetowe, a produkty i usługi, które wytwarza, mogą stanowić istotny towar eksportowy.



Krajowy sektor cyberbezpieczeństwa nie może rozwinąć się bez aktywnego zaangażowania państwa zarówno w domenie cywilnej, jak i wojskowej. Od starannie zaprojektowanej i wdrożonej strategii cyberbezpieczeństwa, poprzez odpowiednie mechanizmy współpracy, do skutecznego programu badań i rozwoju - państwo powinno wspierać rozwój sektora cyberbezpieczeństwa.

Inwestycje realizowane przez PPP są średnio o

15-17 %

tańsze[4]

112

umów zrealizowanych w ramach PPP w Polsce (2009-2016)[5]

5,6

mln PLN wartość zrealizowanych inwestycji[5]

0

liczba inwestycji w obszarze cyberbezpieczeństwa[5]

Państwa, które wybrały taki model rozwoju krajowych sektorów cyberbezpieczeństwa mogą pochwalić się znaczącymi osiągnięciami.

3,75 mld USD
dochód wygenerowany przez izraelski sektor cyberbezpieczeństwa w 2015 r.
(>1% PKB)[7]

2 mld USD + **100,000**
wartość eksportu produktów i usług sektora cyberbezpieczeństwa w Wielkiej Brytanii w 2014 r.[8]
miejsc pracy w sektorze cyberbezpieczeństwa[8]

Polska ma warunki potrzebne do budowy silnego sektora cyberbezpieczeństwa – prężny sektor ICT, wykwalifikowanych inżynierów oraz dynamiczne środowisko akademickie.

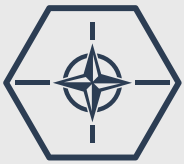
Polski sektor ICT osiągnął wartość
8,5 mld USD
w 2016 r.[9]

Polska zajmuje **3 miejsce** w globalnym rankingu deweloperów[10]

Polskie uniwersytety kształcą **30,000 specjalistów ICT** rocznie.[11]

Ponadto, Polska może korzystać z członkostwa w międzynarodowych organizacjach.

Jako państwo członkowskie UE, Polska może skorzystać z planu inwestycji
1,8 mld EUR
w europejski sektor cyberbezpieczeństwa do 2020 r.



Jako państwo członkowskie NATO Polska może korzystać z takich mechanizmów jak
NATO Industry Cyber Partnership

Cyberprzestrzeń oraz zagrożenia z nią związane stanowią stały element współczesnego świata. Od nas zależy, czy wykorzystamy globalne trendy, czy przegapimy szanse.

Aby jednak w pełni skorzystać z tych możliwości, Polska musi podjąć odpowiednie kroki. Kluczowe rekomendacje płynące z niniejszego raportu to:

ROZWÓJ MECHANIZMÓW WSPÓŁPRACY PUBLICZNO-PRYWATNEJ

- adaptacja istniejących mechanizmów współpracy publiczno-prywatnej (np. partnerstwo publiczno-prywatne) na rzecz projektów związanych z cyberbezpieczeństwem,
- wykorzystanie szans płynących z członkostwa Polski w NATO oraz UE,
- tworzenie nowych mechanizmów, szczególnie na wypadek sytuacji nadzwyczajnych, takich jak bardzo poważny w skutkach cyberatak.

ROZWÓJ MECHANIZMÓW WSPÓŁPRACY SIŁ ZBROJNYCH Z PRYWATNYMI PRZEDSIĘBIORSTWAMI

- rozwój mechanizmów współpracy zarówno na czas pokoju, jak i wojny,
- zaangażowanie utalentowanych inżynierów na potrzeby obronności,
- Tworzenie długoterminowych partnerstw pomiędzy Siłami Zbrojnymi RP a krajowymi firmami ICT.

OPRACOWANIE SKUTECZNEGO PROGRAMU BADAWCZO-ROZWOJOWEGO

- zapewnianie grantów,
- zlecanie działań badawczo-rozwojowych przedsiębiorstwom komercyjnym,
- zapewnianie ulg podatkowych przedsiębiorstwom prowadzącym działalność badawczo-rozwojową.

WSPARCIE I ROZWÓJ RYNKÓW

- wsparcie krajowego rynku produktów i usług cyberbezpieczeństwa poprzez większą otwartość administracji państwowej oraz spółek skarbu państwa na współpracę z krajowymi firmami oraz startupami,
- przeprowadzenie zmian legislacyjnych w celu zwiększenia konkurencyjności krajowych firm ICT (w tym startupów i MŚP) w zamówieniach publicznych,
- pomoc krajowym firmom w dostępie do rynków zagranicznych poprzez przygotowanie i realizację długoterminowej kampanii marketingowej promującej Polskę jako centrum kompetencji w dziedzinie cyberbezpieczeństwa.

1. Abomhara M., Geir M. Køien. 2015. *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks*, "Journal of Cyber Security and Mobility" 2015, 4 (1), pp. 65–88; Camhi J., Business Insider, *BI Intelligence projects 34 billion devices will be connected by 2020*, 2015, [online] www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11?IR=T (access: 12/05/2017).
2. Intel Security, *Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II*, June 2014, [online] https://www.mcafee.com/tw/resources/reports/rp-economic-impact-cybercrime2.pdf (access: 12/05/2017).
3. Cybersecurity Ventures, *2016 Cybercrime Report*, [online] www.cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (access: 12/05/2017).
4. *Value for Money Drivers in the Private Finance Initiative*, Arthur Andersen and Enterprise LSE 2000.
5. The Institute for Public-Private Partnerships, PPP market analysis for the period from 2009 to 31 December 2016.
6. OECD Portal, https://data.oecd.org/rd/gross-domestic-spending-on-r-d.htm (access: 12/05/2017).
7. Israel's National Cyber Bureau data.
8. HM Government, *The UK Cyber Security Strategy 2011-2016: final report.*
9. PMR, *Rynek IT w Polsce 2016. Analiza rynku i prognozy rozwoju na lata 2016-2021, 2016*, [online] www.pmrpublications.com/product/Rynek-IT-w-Polsce-2016 (access: 12/05/2017).
10. HackerRank, *Which Country Would Win in the Programming Olympics?*, 2017, [online] www.blog.hackerrank.com/which-country-would-win-in-the-programming-olympics/ (access: 12/05/2017).
11. Dziennik Internautów Technologie, *Polska kształci za mało informatyków. Umiejętność programowania najbardziej poszukiwaną kompetencją na rynku pracy*, 2015, [online] www.di.com.pl/polska-ksztalci-za-malo-informatykow-umiejetnosc-programowania-najbardziej-poszukiwana-kompetencja-na-rynku-pracy-53442 (access: 12/05/2017).

NA STYKU GOSPODARKI I BEZPIECZEŃSTWA
ADMINISTRACJA PUBLICZNA JAKO KATALIZATOR ROZWOJU NARODOWEGO CYBERBEZPIECZEŃSTWA

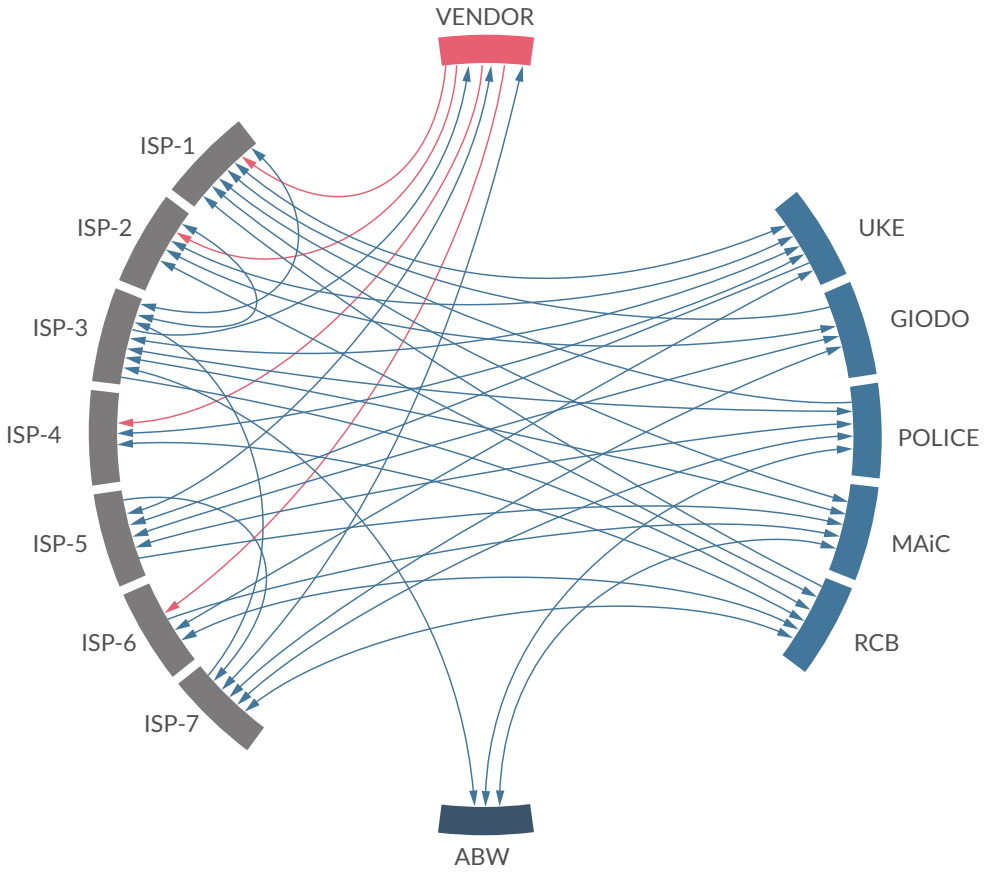
CYPRIAN GUTKOWSKI

Zapewnienie bezpieczeństwa cyberprzestrzeni jest jednym z najważniejszych wyzwań we współczesnym świecie. Problem ten dotyczy bowiem wszystkich, bez wyjątku, począwszy od administracji rządowej i samorządowej, poprzez wszystkie sektory gospodarki, na zwykłym obywatelu, nawet tym, który nie korzysta z komputera, kończąc. Dynamika zmian zachodzących w cyberprzestrzeni zmusza do zwrócenia szczególnej uwagi na jak najlepsze zabezpieczenie zasobów danych. Zabezpieczenie to powinno być uporządkowane i odnosić się do zapewnienia trzech podstawowych cech bezpieczeństwa, tj. poufności, integralności i dostępności (tzw. model CIA – *confidentiality*, *integrity*, *availability*).

Wszelkie działania związane z zapewnianiem cyber-bezpieczeństwa muszą się wpisywać w ustanowiony przepisami prawa ład konstytucyjny i wynikającą z tego ładu odpowiedzialność oraz kompetencje odpowiednich organów władzy publicznej. Trzeba pamiętać jednak, że samo stworzenie przez państwo rozwiązań systemowych i ram prawnych do walki z cyberzagrożeniami to zbyt mało. Konieczna jest współpraca państwa z sektorem

prywatnym. Niedopuszczalna jest sytuacja gdy administracja publiczna ustanawia wiele obowiązków i oczekiwań wobec sektora prywatnego i jednocześnie nie dysponuje ona kompetencjami do współpracy w ich realizacji. Wskazany problem dobrze obrazuje przykład ćwiczeń przeprowadzanych przez Fundację Bezpieczna Cyberprzestrzeń - Cyber-EXE Polska 2014, podczas których operatorzy telekomunikacyjni zobowiązani byli do raportowania zakłóceń bezpieczeństwa do wielu podmiotów administracji państwowej. Niestety mieli problem z uzyskaniem jakiegokolwiek wsparcia tych organów w koordynacji sytuacji kryzysowej[1]. Potrzebny jest w związku z tym rozwój różnych modeli współpracy podmiotów gospodarczych z administracją publiczną w domenie cyberbezpieczeństwa oraz wypracowanie dobrych praktyk.

MAPA RELACJI I WYMIANY INFORMACJI POMIĘDZY SEKTORAMI PUBLICZNYM I PRYWATNYM W CZASIE ĆWICZEŃ CYBER-EXE POLSKA 2014



Budowanie synergii w ramach partnerstwa publiczno-prywatnego[2]

Jedną z potencjalnych form efektywnej współpracy pomiędzy państwem a przedstawicielami sektora prywatnego jest partnerstwo publiczno-prywatne (PPP). Chociaż dotychczas mechanizm ten nie był w Polsce wykorzystywany do przedsięwzięć związanych z dziedziną cyberbezpieczeństwa, to tkwi w nim istotny potencjał. Od 2009 r. do grudnia 2016 r. w ramach partnerstwa publiczno-prywatnego zawarto 112 umów o łącznej wartości 5,6 mld PLN brutto. Niestety nie ma wśród nich ani jednego przykładu współpracy w zakresie zapewnienia cyberbezpieczeństwa instytucji sektora publicznego. Co najwyżej można domniemywać, że cyberbezpieczeństwo jest elementem niektórych projektów. Na liście realizowanych zadań znajdziemy m.in. przedsięwzięcia związane ze świadczeniem usług szerokopasmowego Internetu. Niemniej jednak takich projektów było tylko 13, czyli 11,6% wszystkich zawartych umów, na łączną kwotę 1,9 mld PLN brutto. Z drugiej strony stanowi to aż 34% wszystkich środków przeznaczonych na PPP. Inicjatywa ta, choć cenna i potrzebna z punktu widzenia cyfryzacji kraju, nie dotyka jednak *stricte* kwestii bezpieczeństwa w cyberprzestrzeni RP.

Partnerstwo publiczno-prywatne dzięki łączeniu potencjału podmiotu publicznego i jego partnera prywatnego pozwala efektywniej i skuteczniej tworzyć nową infrastrukturę oraz zwiększać standard i efektywność świadczenia usług publicznych. Od strony administracji publicznej PPP realizowane jest głównie przez samorządy, które zawarły aż 103 ze 112 umów (92%). Administracja rządowa zawarła do końca 2016 r. zaledwie 5 kontraktów (4,5%). Dominująca pozycja samorządów determinuje obecny kształt mechanizmu PPP. Samorządy zainteresowane są realizacją zadań na poziomie lokalnym, natomiast wymiar cyberbezpieczeństwa państwa musi być postrzegany zdecydowanie szerzej.

Zastosowanie mechanizmu PPP w dziedzinie cyberbezpieczeństwa mogłoby przynieść liczne korzyści. Po pierwsze, w przeciwieństwie do klasycznej prywatyzacji usług publicznych, model przedstawiony w PPP pozostawia odpowiedzialność za jakość ich świadczenia po stronie administracji publicznej, zlecając jedynie samo wykonanie zadania podmiotom prywatnym. W przypadku tak wrażliwej sfery jak zapewnienie cyberbezpieczeństwa zasobom państwowym, stanowi to czynnik kluczowy, pozwalający zachować administracji niezbędny zakres zwierzchnictwa nad realizacją prywatyzowanego zadania publicznego. Po drugie, inwestycje realizowane poprzez PPP są tańsze – średnio jest to około 15-17%[3]. Dodatkowo dużo częściej ich realizacja przebiega bez opóźnień w stosunku do przedsięwzięć publicznych wykonywanych samodzielnie przez administrację publiczną i zdecydowanie rzadziej też przekracza zaplanowany budżet[4].

Zalety PPP:

- Mniejsze publiczne wydatki na inwestycje, a przez to oszczędności w budżecie
- Szybsze terminy budowy obiektów użyteczności publicznej i dostaw związanych z nimi usług
- Wyższa jakość usług publicznych
- Większa rywalizacja kapitału prywatnego w sferze dostarczania usług publicznych
- Podział ryzyka inwestycyjnego pomiędzy organ publiczny i prywatnego przedsiębiorcę
- Dodatkowe perspektywy rozwoju dla prywatnych firm

Zalety „partnerstwa doraźnego":

- Elastyczność w określaniu warunków i formuły współpracy
- Możliwość sprawnej alokacji specjalistów na potrzeby działania w sytuacji kryzysowej
- Efektywność kosztowa
- Rozwój dobrych praktyk

Elastyczne formy współpracy

Rozumienie partnerstwa publiczno-prywatnego w zapewnieniu bezpiecznej cyberprzestrzeni nie musi być ograniczane wyłącznie do brzmienia ustawowego, tj. współpracy pomiędzy organami administracji rządowej i samorządowej (administracji publicznej) a podmiotami prywatnymi w oparciu o długoterminowe umowy, których celem jest stworzenie składników infrastruktury umożliwiającej świadczenie usług o charakterze publicznym. Efektem współpracy powinny być także swoiste dobre praktyki postępowania, w tym wymiany informacji i współpracy ze środowiskiem biznesu w przypadku nieprzewidzianego przez umowy cyberzagrożenia. W związku z rozwojem teleinformatyki (ICT) rośnie przecież arsenał cyberprzestępców jak i katalog samych zagrożeń. Niemożliwe jest zatem enumeratywne wyliczenie wszystkich aspektów cyberbezpieczeństwa w katalogu zamkniętym w klasycznej umowie o współpracy cywilnego sektora państwowego z sektorem prywatnym. Konieczne jest stworzenie takich rozwiązań, które umożliwiają sięgnięcie po specjalistów z sektora prywatnego. Może być to narzędzie bardzo istotne w czasie nagłego, pojedynczego, ale niezwykle groźnego dla infrastruktury krytycznej kraju incydentu, wymagającego szybkiego wsparcia eksperckiego dla kadrowych zasobów państwowych.

Administracji publicznej bardzo trudno konkurować z sektorem prywatnym w pozyskiwaniu specjalistów w dziedzinie

cyberbezpieczeństwa. Zgodnie z danymi SANS Institute, płace w tym obszarze w sektorze prywatnym są średnio o ok. 20% wyższe, niż w publicznym[5]. Podobnie wynika z badań GUS, które wskazują, że informatycy zarabiają w urzędach ok. 33% mniej, niż w firmach[6].

Płace w obszarze cyberbezpieczeństwa w sektorze prywatnym są średnio o ok. 20% wyższe, niż w publicznym.

Propozycja doraźnego partnerstwa publiczno-prywatnego, z jednej strony łagodzi wskazane dysproporcje płacowe, pozwala nabywać unikalne doświadczenie „prywatnym" specjalistom oraz zapewnia optymalny poziom cyberbezpieczeństwa zasobom państwowym. Podobne rozwiązanie zastosowano w Estonii, gdzie w ramach partnerstwa publiczno-prywatnego w sytuacji zagrożenia kraju, ochotnicy z sektora prywatnego mają zasilać kadry administracji publicznej – więcej na ten temat znaleźć można w rozdziale drugim. Warto zaznaczyć, że mały kraj jakim jest Estonia na implementację swojej strategii bezpieczeństwa cybernetycznego na lata 2014-2017 wydał 16 mln EUR[7]. Dostosowane do polskich warunków doraźne partnerstwo publiczno-prywatne mogłoby stanowić istotną pomoc dla państwa w czasie kryzysu i zabezpieczałoby państwową infrastrukturę krytyczną w przypadku nagłego i groźnego incydentu. Warto dodać, że w Polsce została już powołana podobna struktura – „Polska Obywatelska Cyberobrona" – która skupia ekspertów (trzecie miejsce na 114 w ćwiczeniach Cyber Europe 2016) gotowych do działań na rzecz państwa.

Przykłady współpracy – polskie doświadczenia

Ciekawym przykładem współpracy jest działające w ramach Naukowej i Akademickiej Sieci Komputerowej (NASK), Narodowe Centrum Cyberbezpieczeństwa (NC Cyber), którego zadaniem jest dbanie o bezpieczeństwo cyberprzestrzeni Rzeczypospolitej poprzez opracowanie narodowych planów ochrony teleinformatycznej. NC Cyber funkcjonuje jako ośrodek wczesnego ostrzegania, który monitoruje i zarządza trybem informowania o zagrożeniach sieciowych. Centrum zajmuje się również obsługą zgłoszeń szkodliwych i nielegalnych treści. Do porozumienia w ramach NC Cyber przystąpiło wiele podmiotów z sektora prywatnego, m.in.: Citi Handlowy, Credit Agricole, mBank, PKO BP, Raiffeisen Polbank, BZW BK, Orange, T-Mobile, Polkomtel, Energa, PSE S.A., Gaz-System S.A., PERN S.A. oraz PKP Informatyka.

Dogodną formułą współpracy publiczno-prywatnej może również być Forum ds. Cyberbezpieczeństwa przy Ministerstwie Cyfryzacji. Zadaniem tego, powołanego w grudniu 2016 r., ciała doradczego miałoby być diagnozowanie potrzeb i ustalanie priorytetów wspólnych działań wszystkich

interesariuszy (w ramach tzw. szerokiego partnerstwa publiczno-prywatnego) krajowego systemu cyberbezpieczeństwa. W ramach Forum powołane zostały grupy eksperckie pracujące nad konkretnymi tematami. Jedną z nich, szczególnie interesującą z punktu widzenia współpracy z sektorem prywatnym, jest zespół do spraw rozwoju NC Cyber. Zebranie w grupie strategicznych podmiotów pozwoli z jednej strony uzyskać wiedzę na temat oczekiwań wobec działalności NC Cyber, z drugiej zaś strony będzie to możliwość zaproponowania pewnych sposobów wymiany informacji i podjęcia współpracy.

Kolejnym przykładem współpracy między sektorem bankowym a administracją jest, zainicjowany przez Ministerstwo Cyfryzacji, Profil Zaufany, dzięki któremu możemy korzystać z platformy Elektroniczna Platforma Usług Administracji Publicznej (ePUAP), umożliwiającej elektroniczny dostęp do urzędów. Dzięki bankowości elektronicznej obywatel może uzyskać swój indywidualny Profil Zaufany, czyli zdobyć elektroniczne potwierdzenie swojej tożsamości za pomocą posiadanego konta bankowego, co w dalszej kolejności pozwala na załatwianie spraw urzędowych przez Internet. Podobny model współpracy zastosowano w programie „Rodzina 500 plus", gdzie na banku ciążyła odpowiedzialność identyfikacji wnioskodawcy i ochrona przed takimi zagrożeniami, jak np. kradzież tożsamości. Jak podaje Ministerstwo Rodziny, Pracy i Polityki Społecznej, na blisko 3 miliony wniosków złożonych w programie, 20% było wnioskami złożonymi online[8]. Do współpracy w ramach tego projektu zgłosiło się 18 banków[9].

Współpraca publiczno-prywatna w świetle Krajowych Ram Polityki Cyberbezpieczeństwa RP

Dotychczasowe działania w obszarze cyberbezpieczeństwa podmiotów ze sfery cywilnej, sektora publicznego i prywatnego oraz instytucji odpowiedzialnych za zwalczanie cyberprzestępczości miały charakter rozproszony, co wpływało na niską efektywność systemu. Obecnie, zgodnie z Krajowymi Ramami Polityki Cyberbezpieczeństwa RP na lata 2017-2022, działania te mają zostać skonsolidowane i zharmonizowane. W programie tym rząd stawia sobie również inne wyzwania, takie jak inwestowanie w rozbudowę zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa poprzez stwarzanie warunków dla rozwoju przedsiębiorstw i startupów oraz ośrodków naukowo-badawczych, których przedmiotem działalności jest tworzenie nowych rozwiązań w obszarze cyberbezpieczeństwa. Działaniom na rzecz rozwoju potencjału narodowego i kompetencji nadano status jednego z celów strategicznych. Dotychczas realizacja wskazanych zadań była uwzględniona wyłącznie w wymiarze technicznym oraz środek konieczny do realizacji zadań w obrębie współpracy na rzecz innowacji czy partnerstwa publiczno-prywatnego. W obecnym brzmieniu, rozwojowi rodzimych zasobów

produktowo-usługowych, wspieraniu działalności badawczo-rozwojowej oraz współpracy publiczno-prywatnej nadano charakter strategiczny, uznając, że mogą one być specjalnością narodową i polskim towarem eksportowym.

Realizowany jest również program rozwojowy Cyberpark Enigma, zakładający m.in. odtworzenie i rozbudowę kompetencji w obszarze produkcji urządzeń i oprogramowania wykorzystywanych we wszystkich gałęziach przemysłu. Oprócz tego ma on zadanie pozyskiwania nowych technologii dla rozwoju rodzimych przedsięwzięć. Według Krajowych Ram Polityki Cyberbezpieczeństwa RP 2017-2022 realizacja tego programu ma nie tylko podnosić poziom odporności na cyberzagrożenia, ale także stanowić istotny bodziec rozwojowy, który ułatwi konkurowanie polskim podmiotom na europejskim rynku specjalistycznych produktów i usług ICT.

Partnerstwo publiczno-prywatne – podejście europejskie

5 lipca 2016 r. Komisja Europejska we współpracy z Europejskim Stowarzyszeniem na rzecz Cyberbezpiezczeństwa (European Cyber Security Association – ECSO) zainauguruwała kontraktowe partnerstwo publiczno-prywatne na rzecz cyberbezpieczeństwa. Jego celem jest pobudzenie inwestycji w dziedzinie cyberbezpieczeństwa w UE, które w perspektywie 2020 r. mają sięgnąć 1,8 mld EUR. Cel ten ma być osiągnięty poprzez odpowiednie alokowanie 450 mln EUR środków europejskich w ramach unijnego programu w zakresie badań naukowych i innowacji „Horyzont 2020". W kontraktowym partnerstwie publiczno-prywatnym na rzecz cyberbezpieczeństwa uczestniczą przedstawiciele biznesu (zarówno dużych korporacji, jak i MŚP), władz krajowych, regionalnych i lokalnych oraz ośrodków badawczych i akademickich.

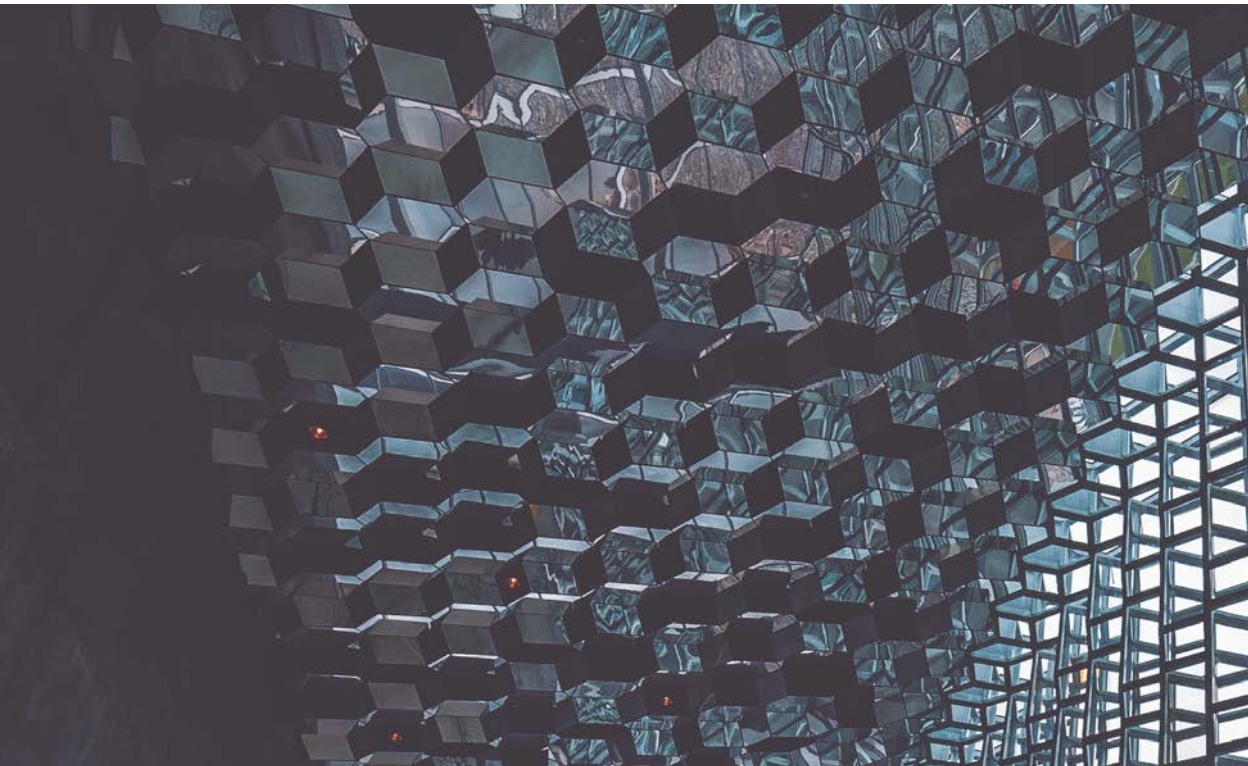
Komisja Europejska we współpracy z Europejskim Stowarzyszeniem na rzecz Cyberbezpiezczeństwa zainauguruwała kontraktowe partnerstwo publiczno-prywatne na rzecz cyberbezpieczeństwa. Jego celem jest pobudzenie inwestycji w dziedzinie cyberbezpieczeństwa w UE, które w 2020 r. mają sięgnąć 1,8 mld EUR.

Partnerstwo powinno się również przyczynić do konsolidacji jednolitego rynku cyfrowego w obszarze cyberbezpieczeństwa. Obecnie, zgodnie z porządkiem traktatowym, na państwach spoczywa obowiązek utrzymania porządku publicznego oraz ochrona bezpieczeństwa narodowego (w tym w cyberprzestrzeni). Konsekwencją takiego stanu rzeczy są różnorodne ograniczenia swobód wolnego rynku czy konkurencji, np. nikły udział w zamówieniach publicznych firm poza krajem macierzystym. Taka fragmentacja unijnego rynku wzmacnia dominację podmiotów spoza

Europy (USA, Azja). W związku z powyższym planowane są różnorodne działania z zakresu konsolidacji jednolitego rynku cyfrowego w obszarze cyberbezpieczeństwa, takie jak np. certyfikacja, walidacja (w tym dla całego sektora ICT), znakowanie (znak jakości bezpieczeństwa/prywatności), zestaw wspólnych specyfikacji przetargów, regulacja, itp.

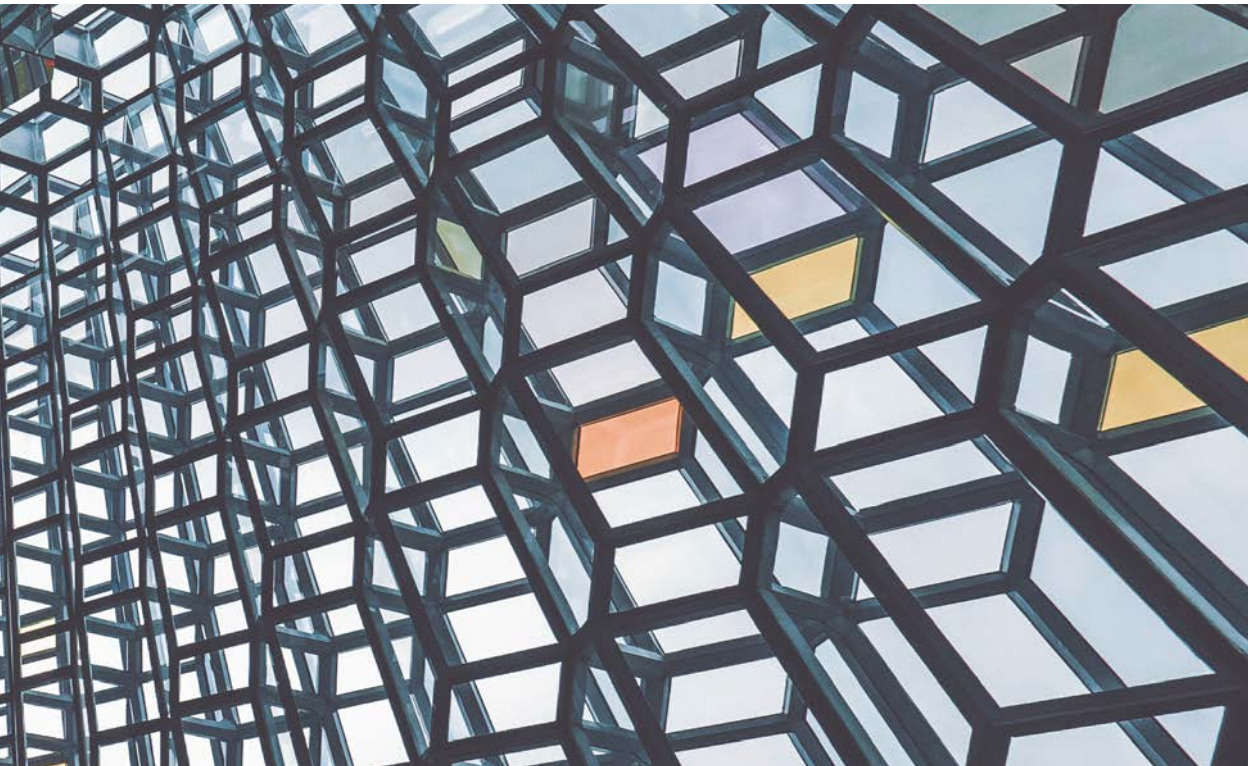
Rozwój dobrych praktyk - konieczny element procesu

Koniecznym jest wypracowanie i przestrzeganie dobrych praktyk postępowania również przy rozpisywaniu i realizacji zamówień publicznych, organizacji przetargów, czy wyborze podwykonawców usług z dziedziny cyberprzestrzeni w dużych instytucjach państwowych (np. ZUS, GIODO, NFZ), czy spółkach skarbu państwa o strategicznym znaczeniu. Państwo powinno wypracować takie ramy prawne, by o cyberbezpieczeństwo dbały wyłącznie sprawdzone i pewne podmioty. Kryterium ceny nie powinno być czynnikiem decydującym. Dużo ważniejsze jest zaufanie i pewność wyboru właściwego partnera, który rzetelnie wykona powierzone zadanie. Zaniedbanie lub dopuszczenie podmiotów nieuprawnionych do zajmowania się bezpieczeństwem ICT może zagrozić bezpieczeństwu państwa.



Sources:

1. Wszystkie wnioski z przebiegu ćwiczeń można znaleźć w Raporcie "Cyber-EXE Polska 2014" pod adresem: https://www.cyberexepolska.pl/wp-content/uploads/2015/01/CYBER-EXE2014_RAPORT-PL.pdf.
2. Na podstawie raportu Instytutu Partnerstwa Publiczno Prywatnego, „Analiza rynku ppp za okres od 2009 do 31 grudnia 2016".
3. Arthur Andersen and Enterprise LSE, "Value for Money Drivers in the Private Finance Initiative".
4. Arthur Andersen and Enterprise LSE, "Value for Money Drivers in the Private Finance Initiative".
5. *Cybrary - Choosing A Career in Cybersecurity: Public Sector or Private Sector?*, https://www.cybrary.it/2015/11/choosing-a-career-in-cybersecurity-public-sector-or-private-sector/.
6. Radzięta S., *Sektor publiczny oszczędza na informatykach*, http://wynagrodzenia.pl/artykul/sektor-publiczny-oszczedza-na-informatykach.
7. *Ministry of Economic Affairs and Communication - Cyber Security Strategy 2014-2017 of Estonia*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Estonia_Cyber_security_Strategy.pdf, s. 13.
8. Związek Banków Polskich – *Raport NetB@nk*, (Q3/2016), https://zbp.pl/wydarzenia/archiwum/konferencje-prasowe/2017/styczen/raport-netb-nk-polacy-maja-juz-33-mln-rachunkow-bankowych-dostepnych-przez-internet.
9. Kancelaria Prezesa Rady Ministrów - Premier Beata Szydło: *18 banków dołącza do przyjaciół programu „Rodzina 500 plus"*, https://www.premier.gov.pl/wydarzenia/aktualnosci/premier-beata-szydlo-18-bankow-dolacza-do-przyjaciol-programu-rodzina-500.html.



CYBEROBRONA I NIE TYLKO
ROLA WOJSKA W BUDOWANIU EKOSYSTEMU CYBERBEZPIECZEŃSTWA W KRAJU

WIESŁAW GOŹDZIEWICZ

Cyberbezpieczeństwo jest zjawiskiem wielopłaszczyznowym i międzysektorowym wymagającym zaangażowania sektora wojskowego i cywilnego, publicznego i prywatnego w celu zwalczania wszelkich możliwych do przewidzenia zagrożeń.

W tym obszarze również istnieje możliwość i potrzeba współpracy z podmiotami sektora przemysłowego i akademickiego jako potencjalnymi dostawcami nowoczesnych rozwiązań w dziedzinie oprogramowania i sprzętu komputerowego. Na świecie istnieją przedsiębiorstwa wyspecjalizowane w dostarczaniu klientom państwowym cybernarzędzi, również tych o charakterze ofensywnym.

Jako element szerzej pojmowanego bezpieczeństwa informacyjnego, cyberbezpieczeństwo będzie się przenikać wzajemnie z innymi obszarami działań, w tym fizycznym bezpieczeństwem infrastruktury sieciowej. Nie jest możliwe uzyskanie cyberbezpieczeństwa bez zapewnienia bezpiecznej łączności, w tym łączności niejawnej (utajonej), a także zbudowania odpowiednio zabezpieczonych sieci teleinformatycznych, zarówno zamkniętych, odizolowanych od Internetu, jak i sieci z Internetem połączonych. W tym drugim przypadku szczególnie istotne są skuteczne zabezpieczenia, w tym diody danych kontrolujące przepływ danych pomiędzy chronioną siecią a Internetem.

POSTANOWIENIA 2 OSTATNICH SZCZYTÓW NATO

SZCZYTY NATO

Newport, 4-5 IX 2014

1. Cyberatak może uruchomić Art. 5 Traktatu Waszyngtońskiego;
2. Prawo międzynarodowe ma zastosowanie w cyberprzestrzeni;
3. Operacje cybernetyczne państw muszą być zgodne z prawem międzynarodowym.

Warszawa, 8-9 VI 2016

1. Cyberprzestrzeń pełnoprawną domeną operacyjną;
2. Członkowie NATO muszą tworzyć skuteczne cybernetyczne zdolności obronne;
3. Cyber Defence Pledge;
4. Obowiązki z Art. 3 Traktatu Waszyngtońskiego obejmują cyberprzestrzeń.

Wszechstronne zdolności cybernetyczne

Cybernetyczne zdolności obronne muszą oczywiście obejmować pasywne środki zabezpieczające wojskową infrastrukturę ICT (lub część cywilnej infrastruktury ICT wykorzystywanej do celów wojskowych) przed niepowołanym dostępem lub wręcz wrogimi działaniami zmierzającymi do zakłócenia funkcjonowania wojskowych systemów ICT, a także umożliwiające bezpieczną, szyfrowaną wymianę informacji pomiędzy uprawnionymi użytkownikami sieci. W interesie resortu obrony leży, aby zarówno systemy zabezpieczające wojskowe sieci przed niepowołanym dostępem bądź próbami włamania do tych sieci, jak i algorytmy szyfrujące były rozwiązaniami unikalnymi, w jak najmniejszym stopniu opartymi na produktach komercyjnych.

Skuteczna obrona – nie tylko w ujęciu cybernetycznym – wymaga posiadania również środków ofensywnych, umożliwiających zarówno prowadzenie aktywnych działań obronnych, jak i przeprowadzenie kontrurderzenia lub – jak kto woli – odwetowego „zhakowania" systemów przeciwnika, a w razie konieczności również przeprowadzenie wyprzedzającego ataku cybernetycznego.

Również Polska mniej lub bardziej otwarcie przyznaje się do poszukiwania ofensywnych zdolności cybernetycznych[1], a w 2013 r. Narodowe Centrum Badań i Rozwoju ogłosiło konkurs na *„Opracowanie oprogramowania i sprzętu do prowadzenia walki informacyjnej* [...]" w tym „[przej*mowania]* kontroli nad urządzeniami sieciowymi [...] oraz [dezintegracji] *węzłów łączności poprzez celową zmianę ich parametrów pracy lub dezaktywację wybranych funkcji."* Dalej czytamy, że *„warunkiem przejęcia elementów sieciowych przeciwnika jest zainstalowanie w nich w sposób jawny lub skryty oprogramowania (malware) i sprzętu elektronicznego* [...]", przewidywano także „[...] *tworzenie własnych botnetów wojskowych* [...][2]". Szacunkowa wartość tego projektu wynosiła ponad 6,5 mln PLN.

Komercyjnie stworzone złośliwe oprogramowanie o nazwie FinFinisher używane jest przez służby specjalne kilku państw, w tym rzekomo również Czech i Słowacji[3], zaś służby specjalne Niemiec przez kilka lat miały korzystać z dostarczonego komercyjnie malware, któremu przypisano nazwę R2D2[4].

W projektowanym na lata 2017-2022 Planie Modernizacji Technicznej (PMT) Sił Zbrojnych przewiduje się, że zarówno w latach 2017-2019, jak i w całym pięcioletnim okresie objętym PMT, na rozwój zdolności cybernetycznych polskie wojsko przeznaczy 1% całości środków PMT, czyli łącznie około 1 mld PLN. Nominalnie kwota ta wygląda imponująco, choć nieco błędnie w zestawieniu ze środkami przeznaczonymi na inne programy priorytetowe, jak np. modernizację obrony powietrznej przeznaczone zostanie w latach 2017-2019 14% wartości PMT, a w całym pięcioletnim okresie – 24%, a na rozwój wojsk pancernych i zmechanizowanych, odpowiednio 20% i 14%[5].

Budowanie wojskowych zdolności – komercjalizacja i współpraca

Stworzenie skutecznego potencjału cybernetycznego wymaga szeroko pojętej współpracy resortu obrony i sił zbrojnych, zarówno wewnętrznej, jak i międzynarodowej. Konieczne jest stworzenie mechanizmów koordynacji działań i wymiany informacji z cywilnymi organami i podmiotami zaangażowanymi w obronę cybernetyczną państwa, w tym również podmiotami sektora prywatnego, w szczególności operatorami systemów infrastruktury krytycznej.

Wagę takiej współpracy doceniło już wiele państw. Dla przykładu estońska Strategia Bezpieczeństwa Cybernetycznego na lata 2014-2017 przewiduje stworzenie warunków do organizacji i przeprowadzanie szkoleń, warsztatów i badań naukowych w dziedzinie cyberbezpieczeństwa, a także zintensyfikowanie działań międzysektorowych. Ponadto, dokument ten uznaje, że współpraca między sektorami publicznym, prywatnym i akademickim, biorąc pod uwagę wzajemne zależności i połączenia (również fizyczne, sieciowe) infrastruktury i usług ICT, jest niezbędna dla budowania cyberbezpieczeństwa w sposób skoordynowany[6].

Podobne tezy formułuje również francuska strategia bezpieczeństwa cyfrowego, która ponadto wprost, podobnie jak niniejsze opracowanie, sugeruje, iż dla zapewnienia cyfrowej suwerenności państwa niezbędne jest wspieranie konkurencyjności jego krajowego sektora przemysłowego i naukowego w dziedzinie cyberbezpieczeństwa. Francja ma wspierać tworzenie środowiska przyjaznego badaniom i innowacjom poprzez między innymi mobilizację i koordynację wszystkich dostępnych zasobów, publicznych i prywatnych, w celu zapewnienia francuskim rozwiązaniom w dziedzinie cyberbezpieczeństwa przewagi konkurencyjnej, co w konsekwencji przyniesie wymierne korzyści nie tylko sektorowi prywatnemu, ale i całemu państwu[7].

Wzorcem dla współpracy z sektorem akademickim i przemysłowym może być NATO-Industry Cyber Partnership (NICP), oparte na słusznym założeniu, że ścisła współpraca pomiędzy zamawiającym (NATO) a dostawcą (przemysł) jest kluczem do sprawnego tworzenia rozwiązań w dziedzinie cyberbezpieczeństwa, a uwzględnienie w tej współpracy sektora akademickiego zaowocuje dostępem do najnowszych osiągnięć naukowych i technologicznych.

NICP zrzesza instytucje NATO, narodowe CERTy, a także przedstawicieli sektora przemysłowego z państw członkowskich NATO, w tym średnie i małe przedsiębiorstwa z branży ICT, a także ośrodki akademickie. Wszystkie te podmioty łączą wspólne dla nich zagrożenia i wyzwania w dziedzinie bezpieczeństwa, a także założenie, że współpraca i wymiana informacji, w szczególności w zakresie najnowszych rozwiązań stanowiących wynik prac badawczo-rozwojowych prowadzonych już przez przedsiębiorstwa i ośrodki naukowe, mogą znacznie przyspieszyć osiągnięcie przez NATO pożądanych zdolności w obszarze obrony cybernetycznej[8].

W ramach NICP stworzono między innymi Cyber Information and Incident Coordination System (CIICS), którego opracowanie NATO Communications and Information Agency (NCIA) powierzyła Rhea Group, belgijskiej spółce zależnej kanadyjskiej ADGA Group[9]. Warto podkreślić, że NCIA dysponuje rocznym budżetem rzędu 600 mln EUR na projekty związane z infrastrukturą ICT[10], a między 2016 a 2019 r. planuje przeznaczyć łącznie około 3 mld EUR na rozmaite projekty w dziedzinie technologii informacyjnych na potrzeby między innymi systemów dowodzenia i kierowania, łączności satelitarnej, systemów obrony powietrznej i obrony cybernetycznej[11].

Możliwe kierunki współpracy publiczno-prywatnej

Współpraca między podmiotami sektora publicznego, prywatnego i akademickiego może umożliwić skrócenie czasu trwania prac badawczo-rozwojowych, jeżeli stworzy się mechanizmy wymiany i dzielenia się informacjami.

Mechanizmy takie w ramach NICP funkcjonują na podstawie porozumień w zakresie partnerstwa przemysłowego (*Industry Partnership Agreements* – IPAs), jakie NCIA zawiera z podmiotami sektora przemysłowego. Porozumienia takie NCIA zawarła między innymi z FireEye czy RSA Security. Celem IPA jest umożliwienie szybkiej wymiany informacji o cyberzagrożeniach w celu poprawy świadomości sytuacyjnej stron porozumienia i wzmocnienia ochrony ich sieci.

Wzajemne korzyści ze współpracy podmiotów wojskowych z partnerami przemysłowymi i akademickimi są nie do przecenienia, w szczególności, jeżeli współpraca ta obejmuje podmioty krajowe.

- Po pierwsze, umożliwi zasilenie krajowych przedsiębiorstw i ośrodków akademickich środkami na prowadzenie prac badawczo-rozwojowych i wdrożeniowych ukierunkowanych na tworzenie rozwiązań zamawianych przez resort obrony.

- Po drugie, zapewni możliwość dostosowania rozwiązań opracowywanych przez podmioty sektora przemysłowego i akademickiego do specyficznych potrzeb zamawiającego.

- Po trzecie – i temu aspektowi należy poświęcić szczególną uwagę – może przyczynić się do zwiększenia bezpieczeństwa projektowanych rozwiązań i systemów.

Poleganie na krajowych podmiotach sektora przemysłowego i akademickiego w rozwijaniu zdolności cybernetycznych, w szczególności, jeżeli chodzi o rozwiązania kryptologiczne i kryptograficzne, umożliwi stworzenie rozwiązań prawdziwie bezpiecznych, np. poprzez

PRZYKŁADY ZAMÓWIEŃ Z OBSZARU OBRONY CYBERNETYCZNEJ OBEJMUJĄ:

- Implementację pełnej zdolności operacyjnej NATO Computer Incidents Response Capability (NCIRC); kontrakt o wartości 134.353,77 EUR przyznany SELEX Communications SpA;
- Implementację interfejsu NCIRC w jednostce obrony przeciwrakietowej w Ramstein; kontrakt o wartości 411.173,64 EUR przyznany SELEX Communications SpA;
- Instalację systemu zabezpieczeń elektronicznych sieci aktywnej (Active Network Electronic Security System – ANWI ESS) dla NCIRC; kontrakt o wartości 352.166,22 EUR przyznany SELEX SpA;
- Odnowienie licencji Trend Micro dla NCIRC; kontrakt o wartości 101.481,02 EUR przyznany- Insight Technology Solutions Belgium, Inc;
- Odnowienie licencji McAffee dla NCIRC, kontrakt o wartości 498.627,34 EUR przyznany UNI BUSINESS CENTRE B.V.;
- Centralny zakup stacji roboczych z certyfikatami TEMPEST poziomu B; kontrakt o wartości 1.662.375,58 EUR przyznany Airbus Defence and Space AS.;
- Zakup sprzętu łączności i informatyki na potrzeby Jednostek Integracji Sił NATO (NATO Force Integraton Units – NFIUs); kontrakt o wartości 2.762.779,00 EUR przyznany Airbus Defence and Space AS.;
- Zakup sprzętu kryptograficznego dla infrastruktury komunikacyjnej NATO; kontrakt o wartości 941.334,89 EUR przyznany Thales Norway AS12[12].

takie ukształtowanie warunków zamówienia, aby autor rozwiązań udostępnił zamawiającemu kody źródłowe, a jednocześnie zobowiązał się do udostępnienia stworzonych rozwiązań wyłącznie zamawiającemu, tak aby tylko on miał możliwość użytkowania danych rozwiązań . Najważniejszym aspektem jest tu uniezależnienie się od produktów komercyjnych, dostępnych powszechnie, w których niejednokrotnie występują luki zabezpieczeń, nierzadko celowo pozostawione przez producenta, jak to miało miejsce np. w przypadku systemu RCS zakupionego przez służby specjalne szeregu państw, w tym polskie Centralne Biuro Antykorupcyjne. Autorzy rozwiązań komercyjnych niechętnie (o ile w ogóle) udostępniają klientom kody źródłowe oprogramowania, nierzadko sprzedając je jako tzw. „black box" bez możliwości dokonywania modyfikacji czy usprawnień przez użytkownika. Brak dostępu do kodów źródłowych może skutecznie uniemożliwić zidentyfikowanie ewentualnych luk w zabezpieczeniach i ich wyeliminowanie.

Jak rekrutować cyberżołnierzy?

Nie można myśleć o zbudowaniu potencjału w zakresie cyberbezpieczeństwa bez wykorzystania kapitału ludzkiego, jakim dysponuje państwo. W ograniczonym jedynie zakresie kapitał ludzki będzie w „posiadaniu" struktur wojskowych – zdecydowana większość specjalistów w dziedzinie cyberbezpieczeństwa będzie „wchłaniana" przez sektor cywilny, gdzie popyt na tych specjalistów jest właściwie nieograniczony. Należy zatem stworzyć systemowe rozwiązania umożliwiające przyciągnięcie specjalistów do instytucji państwowych, w tym wojskowych, bądź też np. objęcie takich specjalistów swoistymi przydziałami mobilizacyjnymi na wypadek kryzysu lub konfliktu zbrojnego, kiedy niezbędne stanie się wzmocnienie potencjału obronnego państwa, w tym cybernetycznego potencjału wojskowego. Za przykład takich rozwiązań posłużyć może włączenie Jednostki Obrony Cybernetycznej Estońskiej Ligi Obronnej do systemu obrony narodowej i objęcie całej Estońskiej Ligi Obronnej na wypadek konfliktu statusem analogicznym do statusu przysługującego Siłom Zbrojnym Estoni[13] czy stworzenie Obywatelskiej Rezerwy Cybernetycznej (*Reserve Citoyenne Cyber*) we Francji[14].

Na przeciwległym biegunie znajduje się Izrael. Jego Siły Obronne do tej pory opierają się na powszechnym poborze, który obejmuje również kobiety. Jednostka 8200, powołana między innymi do prowadzenia operacji cybernetycznych, skupia specjalistów pełniących zarówno służbę zawodową, jak i zasadniczą. Były dowódca jednostki i jednocześnie jej twórca, gen. bryg. Danny Bren spytany o kapitał ludzki i przepaść płacową pomiędzy oficerami i podoficerami zajmującymi się cyberoperacjami stwierdził, iż główną motywacją do pozostania w służbie w Jednostce 8200 jest mimo wszystko chęć sprostania wyzwaniom, jakie służba ta oferuje. Porównał również Jednostkę 8200 do startupu, w którym rolę inwestora pełnią Izraelskie Siły Obronne[15].

Siły Obronne Izreala przeczesują uczelnie w poszukiwaniu młodych kandydatów do służby w Jednostce 8200, cechujących się wyjątkowymi umiejętnościami analitycznymi, ale jednocześnie potrafiących pracować zespołowo. W ramach obowiązkowej służby wojskowej, zamiast uczyć się musztry, obsługi broni czy taktyki, przechodzili przeszkolenie w klimatyzowanych wygodnych pomieszczeniach Jednostki 8200 ucząc się zbierania informacji wywiadowczych, korzystania z najnowszych osiągnięć zwiadu elektronicznego czy technik *data-mining*. Byli żołnierze Jednostki 8200 , również dzięki przeszkoleniu w Jednostce 8200 często osiągali sukcesy na rynku[16]. Stoją za stworzeniem takich przedsiębiorstw, jak Check Point, CloudEndure, CyberReason, ICQ, LightCyber, NSO Group, Palo Alto Networks, indeni, NICE, AudioCodes, Gilat, outbrain, Leadspace, EZchip, Onavo, Singular, CyberArk, czy Fortscale. Izraelskie wojsko zainwestowało w swoich specjalistów, którzy dzięki wiedzy zdobytej w Jednostce 8200 niejednokrotnie odnieśli sukcesy w biznesowej działalności na polu cyberbezpieczeństwa, a jednocześnie pozostają na tzw. przydziałach mobilizacyjnych i regularnie powoływani są na ćwiczenia rezerwy, podczas których wykorzystują wiedzę i doświadczenie zdobyte zarówno podczas służby wojskowej, jak i w późniejszej działalności gospodarczej.

Oczywiście rozwiązania takie będą wymagały również stworzenia odpowiedniego systemu szkolenia umożliwiającego cywilnym specjalistom względnie bezproblemowe wdrożenie się do działania w zhierarchizowanych strukturach państwowych. Jednym z możliwych rozwiązań jest ogłoszenie ochotniczego „naboru" specjalistów do udziału w ćwiczeniach i treningach, tak wojskowych, jak i cywilnych ćwiczeniach reagowania (zarządzania) kryzysowego. Biorąc pod uwagę poziom wynagrodzeń w resorcie obrony narodowej, z dużym prawdopodobieństwem można założyć, iż motywacja finansowa w większości przypadków nie będzie głównym czynnikiem branym pod uwagę przez cywilnych specjalistów podejmujących decyzję o zaangażowaniu się w działania na rzecz wzmocnienia cyberbezpieczeństwa państwa. Maksymalne wynagrodzenie pracownika cywilnego resortu, zgodnie z postanowieniami Ponadzakładowego Układu Zbiorowego Pracy dla Pracowników Wojskowych Jednostek Organizacyjnych Sfery Budżetowej[17] wynosi 8000 PLN brutto, choć biorąc pod uwagę hierarchię stanowisk cywilnych w MON, trudno oczekiwać, że cyberspecjaliści otrzymywać będą właśnie tę najwyższą stawkę wynagrodzenia.

Wynagrodzenia dla rezerwistów powoływanych na ćwiczenia wojskowe również nie prezentują się szczególnie atrakcyjnie. Wynagrodzenie netto za 30-dniowe ćwiczenia wyniesie 2100 PLN dla szeregowego, 2512,50 PLN dla plutonowego i 3150 PLN dla podporucznika. Żołnierz rezerwy w stopniu podpułkownika otrzyma za 30-dniowe ćwiczenie około 5600 PLN[18], a dla przykładu jego niemiecki odpowiednik około 3500 EUR plus dodatki, w tym za posiadanie kwalifikacji

WYNAGRODZENIA NETTO ZA TRZYDZIESTODNIOWE ĆWICZENIA

i umiejętności szczególnie przydatnych dla wojska. Wynagrodzenia i uposażenia oferowane przez polski resort obrony narodowej nie są konkurencyjne w porównaniu z ofertą sektora prywatnego, co podkreślane było wielokrotnie (również przez przedstawicieli administracji rządowej) podczas Polskiego Forum Cyberbezpieczeństwa w 2016 r.[19] i Europejskiego Forum Cyberbezpieczeństwa w 2015 r[20].

Wartym rozważenia jest poszukiwanie młodych specjalistów, którzy wyróżnią się w różnych konkursach czy hackathonach, tym samym potwierdzając swoją wiedzę i umiejętności przydatne z punktu widzenia cyberbezpieczeństwa. Jednym z możliwych rozwiązań jest zwiększenie liczby tego typu przedsięwzięć zarówno o charakterze krajowym, jak i międzynarodowym[21].

W celu maksymalnego wykorzystania kapitału ludzkiego bez „wyrywania" go ze środowiska pracy, można rozważyć współpracę z przedsiębiorcami wyspecjalizowanymi w dziedzinie cyberbezpieczeństwa, którzy skłonni byliby zaoferować swój potencjał na rzecz wzmocnienia zdolności obrony cybernetycznej państwa poprzez udział w odpowiednich ćwiczeniach. Znane są przypadki powierzania przez ministerstwa obrony przedsiębiorstwom prywatnym przeprowadzenia testów zabezpieczeń, w tym testów penetracyjnych. Można również wziąć pod uwagę skorzystanie z potencjału przedsiębiorców zrzeszonych w inicjatywach na wzór Polskiej Obywatelskiej Cyberobrony, poprzez zarówno włączenie ich do międzyresortowych i międzysektorowych ćwiczeń w zakresie bezpieczeństwa cybernetycznego, jak i zlecanie im prowadzenia testów penetracyjnych, symulowanych ataków cybernetycznych na systemy teleinformatyczne lub wręcz opracowywania skutecznych metod i technik zabezpieczenia kluczowych systemów ICT, w oparciu o doświadczenie pozyskane przez przedsiębiorców pozyskane odpieranie ataków cybernetycznych na ich własne systemy.

ŹRÓDŁA

1. *Doktryna cyberbezpieczeństwa Rzeczypospolitej Polskiej*, Biuro Bezpieczeństwa Narodowego, 22 stycznia 2015, ISBN: 978-83-60846-25-4, s. 9.
2. http://www.ncbir.pl/gfx/ncbir/pl/defaultopisy/575/6/1/polaczony.pdf, s. 42.
3. *WikiLeaks ujawnia klientów rządowego szpiegowskiego oprogramowania FinFisher*, [online] https://niebezpiecznik.pl/post/wikileaks-ujawnia-klientow-rzadowego-szpiegowskiego-oprogramowania-finfisher/?similarpost.
4. *Niemiecka policja infekuje rządowym trojanem (R2D2)*, [online] https://niebezpiecznik.pl/post/niemiecka-policja-infekuje-rzadowym-trojanem-r2d2/.
5. Tomasz Dmitruk, *Projekt nowego Planu Modernizacji Technicznej*, [online] http://dziennikzbrojny.pl/artykuly/art,2,4,10262,armie-swiata,wojsko-polskie,projekt-nowego-planu-modernizacji-technicznej.
6. *Cyber Security Strategy 2014-2017*, Estonian Ministry of Economic Affairs and Communication, s. 7.
7. *French National Digital Security Strategy*, Agence nationale de la sécurité des systèmes d'information (ANSSI) 2015,[online] https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf, s. 30-31.
8. *Who will be involved in the NATO Industry Cyber Partnership?*, [online] http://www.nicp.nato.int/nicp-stakeholders/index.html.
9. Brooks Tigner, *NATO tests cyber alerting tool*, [online] http://www.nicp.nato.int/nato-tests-cyber-alerting-tool/index-2.html.
10. *Why bidding on NATO contracts can boost your bottom line*, [online], http://tradecommissioner.gc.ca/canadexport/157947.aspx?lang=eng.
11. *NATO announces 3 billion EUR investment in defence technology*, [online] https://www.ncia.nato.int/NewsRoom/Pages/160726_Announcement_3billion_investments.aspx.
12. Opracowano na podstawie ogłoszeń o udzieleniu zamówień publikowanych na stronie https://www.ncia.nato.int/Industry/Pages/NCI-Agency-Procurement.aspx.
13. *The Estonian Defence League Act*, [online] https://www.riigiteataja.ee/en/eli/525112013006/consolide.
14. *Réserve citoyenne cyber: une démarche originale*, [online] http://www.defense.gouv.fr/actualites/communaute-defense/reserve-citoyenne-cyber-une-demarche-originale/(language)/fre-FR.
15. Israel Wulman, *IDF unveils new cyber defense HQ*, [online] http://www.ynetnews.com/articles/0,7340,L-4820035,00.html.
16. Idan Tendler, *From The Israeli Army Unit 8200 To Silicon Valley*, [online] https://techcrunch.com/2015/03/20/from-the-8200-to-silicon-valley/.
17. http://www.wbe.wp.mil.pl/plik/file/akty/oslony/akt_199.pdf.
18. http://sandomierz.wku.wp.mil.pl/pl/7373.html.
19. *CYBERSEC PL 2016 Rekomendacje*, [online] https://cybersecforum.pl/files/2016/06/rekomendacje_cspl2016_pl.pdf, s. 3-4, 10-11.
20. CYBERSEC 2015 Rekomendacje, {online] https://app.box.com/s/o0nb9edtybgxqo9apkjxuium2m6vq9gy, s. 12, 16, 21.
21. *Ibidem*, s. 21.

ROZWÓJ INNOWACYJNOŚCI STUDIUM PRZYPADKÓW WSPÓŁPRACY PUBLICZNO-PRYWATNEJ W WYBRANYCH PAŃSTWACH

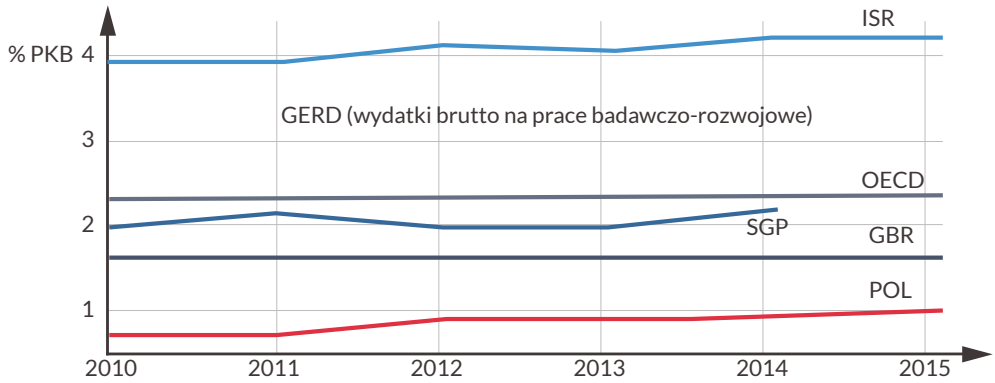
LIOR TABANSKY

Skuteczne budowanie cyberbezpieczeństwa wymaga innowacji – przede wszystkim ze względu na to, że nowe wyzwania powstają z prędkością określoną prawem Moore'a (moc obliczeniowa komputerów podwaja się co dwa lata). Innowacje z reguły są wynikiem prac badawczo-rozwojowych (B+R)[1]:

WYTYCZNE OECD W ZAKRESIE ZBIERANIA I RAPORTOWANIA DANYCH DOTYCZĄCYCH BADAŃ I ROZWOJU EKSPERYMENTALNEGO

Podczas gdy sektor prywatny przeprowadza zdecydowaną większość badań stosowanych i eksperymentalnych prac rozwojowych w zakresie technologii ICT, środowisko akademickie odpowiada za badania podstawowe. Innowacyjność zależy więc od współpracy

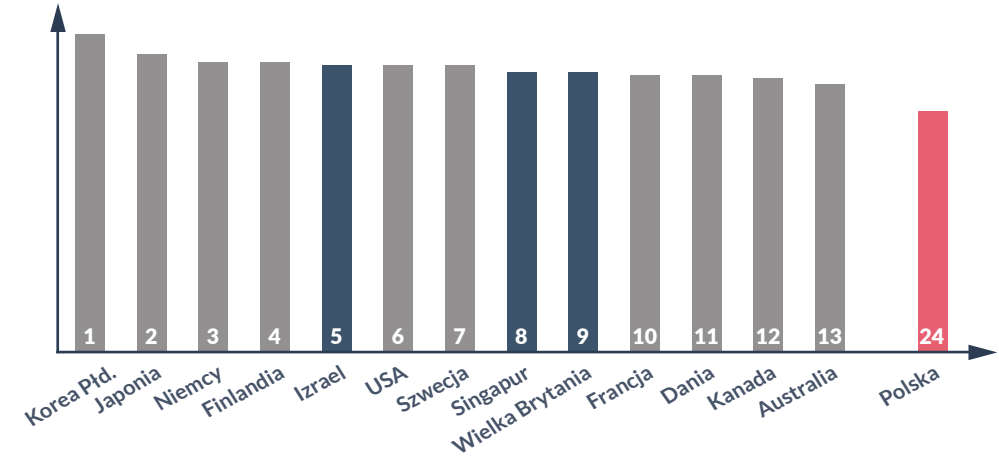
INTENSYWNOŚĆ PRAC BADAWCZO-ROZWOJOWYCH W OECD ORAZ W WYBRANYCH GOSPODARKACH[3]



administracji publicznej, biznesu i środowiska akademickiego. Powyższą relację dobrze oddaje koncepcja Narodowego Systemu Innowacji (*National Innovation System*), która narodziła się pod koniec lat 80. XX w. w ekonomii i zarządzaniu. Umożliwia ona analizę całego szeregu interesariuszy oraz ich interakcji[2]. Powszechnym wskaźnikiem innowacyjności są wydatki na prace badawczo-rozwojowe (B+R) jako procent produktu krajowego brutto (PKB).

W niniejszym rozdziale przeanalizowano trzy przypadki współpracy sektora publicznego i prywatnego dla innowacji w dziedzinie cyberbezpieczeństwa. Wybrane państwa – Izrael, Wielka Brytania oraz Singapur – plasują się wśród 10 wiodących gospodarek innowacyjnych (5, 8, 10), stanowiąc dobry punkt odniesienia dla Polski, która zajmuje 24 miejsce[4].

RANKING BLOOMBERG INNOVATION INDEX 2015[4]



IZRAEL
JAK STAĆ SIĘ ŚWIATOWĄ CYBERPOTĘGĄ W 5 LAT

W ostatnich latach Izrael stał się jedną z wiodących cyberpotęg na świecie[5].

Od 2014 r. w Izraelu powstało ponad 100 nowych firm sektora cyberbezpieczeństwa. W tym czasie zainwestowano niemal 400 mln USD w 78 spośród nich. Dyrektor Izraelskiego Narodowego Biura Cyberbezpieczeństwa (*Israel National Cyber Bureau* – INCB) oznajmił 15 lutego 2015 r. podczas zebrania rządu, że izraelski przemysł cyberbezpieczeństwa zanotował w 2014 r. rekordowe osiągnięcia.

- Około 30 startupów zebrało ponad 200 mln USD – to wzrost o 40% w porównaniu z 2013 r.

- Osiem izraelskich firm z branży cyberbezpieczeństwa zostało zakupionych przez inwestorów zagranicznych za łączną kwotę ok. 700 mln USD[6].

Eksport izraelskich spółek z branży cyberbezpieczeństwa oszacowano na ok. 3 mld USD w 2013 r., co trzykrotnie przewyższa eksport Wielkiej Brytanii w tym sektorze. Jak informował *The Economist*, rozmiar izraelskiego eksportu w zakresie produktów i usług cyberbezpieczeństwa wzrósł do 6 mld USD w 2014 r. i pod tym względem ustępuje tylko USA[7]. Izrael obecnie przyciąga około 15-20% globalnych inwestycji rynkowych w badania i rozwój w dziedzinie cyberbezpieczeństwa. Tel Awiw jest siedzibą od 3 100 do 4 200 aktywnych startupów technologicznych i plasuje się na piątym miejscu na świecie w rankingu najlepszych miast dla startupów, będąc pierwszym spośród miast leżących poza USA[8].

250
Liczba izraelskich przedsiębiorstw sektora cyberbezpieczeństwa

5
Liczba ośrodków badań nad cyberbezpieczeństwem

$3,5–$4mld
Sprzedaż izraelskiego sektora cyberbezpieczeństwa w 2015 r.

20%
Globalny udział inwestycji sektora prywatnego w cyberbezpieczeństwo

100%
Wzrost udziału inwestycji w cyberbezpieczeństwo w porównaniu z 2014 r.

Są to wyniki wysiłków w zakresie polityki, w tym wsparcia sektora przedsiębiorstw przez rząd w dziedzinie tworzenia i wdrażania innowacji.

W 2010 r. Premier Netanjahu powołał komisję ekspertów w ramach Narodowej Inicjatywy Cyberbezpieczeństwa (*National Cyber Initiative* – NCI) powierzając jej ewaluację stanu cyberbezpieczeństwa i polityki Izraela w tym zakresie. Kluczowym zadaniem komisji było zbadanie w jaki sposób stworzyć zachęty dla rozwoju sektora cyberbezpieczeństwa w Izraelu, aby do 2015 r. zapewnić mu miejsce wśród pięciu najlepiej rozwiniętych w tej dziedzinie krajów[9].

80 ekspertów ze wszystkich branż pracowało przez sześć miesięcy w ośmiu podkomisjach. Główną rekomendację powstałą w wyniku ich pracy można streścić jako zwiększenie współpracy rządu, sił zbrojnych, środowiska akademickiego i przemysłu w Izraelu.

W Uchwale Rządu nr 3611 z dnia 7 sierpnia 2011 r. pt. „Rozwój narodowych zdolności w cyberprzestrzeni”[10] przyjęto zalecenia Narodowej Inicjatywy Cyberbezpieczeństwa, a dokument ten stanowi krajową strategię cyberbezpieczeństwa Izraela.

Kładąc nacisk na potrzebę zwiększenia intensywności badań i rozwoju sektora cyberbezpieczeństwa, INCB jest odpowiedzialne za realizację następujących zadań:

- promocja prac badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa
- wzmocnienie sektora cyberbezpieczeństwa w Izraelu w oparciu o eksport

Obecnie pięć z siedmiu uniwersytetów w Izraelu utworzyło ośrodki badań nad cyberbezpieczeństwem wspierane przez INCB. Interdyscyplinarne Centrum Badań nad Cyberbezpieczeństwem im. Leonarda Bławatnika na Uniwersytecie Telawiwskim (*Tel Aviv University's Blavatnik Interdisciplinary*

> ***[Należy] wzmocnić ochronę infrastruktury krajowej, koniecznej dla utrzymania stabilnej i produktywnej gospodarki w Izraelu oraz w możliwie największym stopniu uodpornić tę infrastrukturę na cyberataki przez rozwój Izraela jako centrum kompetencji ICT, równocześnie wspierając współpracę środowiska akademickiego, przemysłu, sektora prywatnego, agencji rządowych i organów specjalnych***
>
> Rekomendacje zawarte w Uchwale Rządu nr 3611 z dnia 7 sierpnia 2011 r. pt. „Rozwój narodowych zdolności w cyberprzestrzeni”

Cyber Research Centre – TAU ICRC) otwarte we wrześniu 2014 r. stanowi pierwszy przykład zinstytucjonalizowanej współpracy rządu izraelskiego ze środowiskiem akademickim w dziedzinie badań nad cyberbezpieczeństwem. INCB finansuje niemal połowę budżetu na badania, lecz alokacja funduszy pozostaje niezależna i podlega standardowemu akademickiemu kryterium doskonałości naukowej. Rząd wstrzymuje się od zarządzania procesami innowacji. Oprócz działalności w dziedzinie nauk ścisłych i inżynierii, TAU ICRC prowadzi również badania z zakresu nauk politycznych i społecznych.

Za pośrednictwem INCB rząd koordynuje rozwój sektora cyberbezpieczeństwa, a głównym realizowanym obecnie projektem jest utworzenie dodatkowego klastra cyberbezpieczeństwa w Beer Szewie, który skupia jednostki wywiadu wojskowego i militarne jednostki technologiczne, rządowy CERT, Uniwersytet Ben-Guriona, a także prywatne przedsiębiorstwa. W celu zachęcenia przedsiębiorstw do lokowania swojej działalności w tym klastrze, rząd zapewnia infrastrukturę i zachęty ekonomiczne, takie jak np. refundacja do 20% wynagrodzenia każdego pracownika zatrudnionego w obszarze cyberbezpieczeństwa[11].

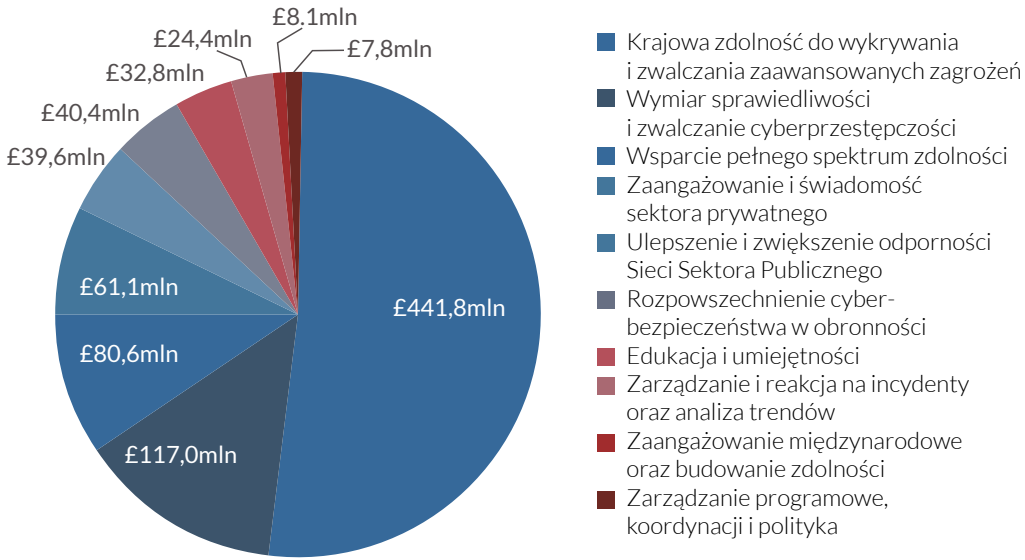
WIELKA BRYTANIA
NUMER 1 SEKTORA CYBERBEZPIECZEŃSTWA W EUROPIE

Strategia cyberbezpieczeństwa Wielkiej Brytanii została opublikowana w listopadzie 2011 r., zaraz po dokumencie izraelskim[12]. Strategia brytyjska odnosiła się nie tylko do bezpieczeństwa, ale także do aspektów gospodarczych. Dokument wskazywał cel 2 mld GBP w eksporcie produktów i usług sektora cyberbezpieczeństwa, który miał być osiągnięty do końca 2016 r. Należy stwierdzić, że cel strategii na lata 2011-2016 został w znacznym stopniu zrealizowany, dzięki wszechstronnej współpracy przemysłu, środowiska akademickiego i partnerów międzynarodowych:

- W zakresie ochrony krajowej infrastruktury krytycznej rząd współpracował z właścicielami i operatorami poprzez wdrażanie planów zarządzania ryzykiem w sieci[13].

- Przedsiębiorstwom ze wszystkich sektorów bez względu na rozmiar prowadzonej działalności (mikro, małe, średnie i duże) oferowano wsparcie w zakresie usług doradztwa i szkoleń dotyczących zarządzania ryzykiem w zakresie cyberbezpieczeństwa, np. w postaci programu „Podstaw cyberbezpieczeństwa" (*Cyber Essentials Scheme*)[14].

BRYTYJSKA STRATEGIA BEZPIECZEŃSTWA CYBERNETYCZNEGO NA LATA 2011–2016 Z PODZIAŁEM NA OBSZARY TEMATYCZNE



Cel 7.2.3. Brytyjskej Strategii bezpieczeństwa cybernetycznego na lata 2011-2016:

- **zapewnianie zaplecza badawczego dla przedsiębiorstw rozwijających swoje produkty, wraz z szybką ścieżką oceny dla nowych produktów i usług w dziedzinie cyberbezpieczeństwa;**
- **czerpanie ze wspólnej fachowej wiedzy publiczno-prywatnego Partnerstwa dla Rozwoju Cyberbezpieczeństwa, aby kształtować oraz nakierowywać dalszy rozwój innowacji;**
- **pomoc przedsiębiorstwom bez względu na rozmiar w rozwoju i dostępie do rynków międzynarodowych.**

- Brytyjskie firmy sektora cyberbezpieczeństwa zwiększyły swój udział w globalnym rynku[15]. Cały sektor odnotował wzrost z10 mld GBP do ponad 17 mld GBP i wykazuje zatrudnienie na poziomie 100 tys. osób. Udział brytyjskiego eksportu w dziedzinie cyberbezpieczeństwa w skali globalnej wzrósł z 3,6% do 4,4%, co stanowi 1,47 mld GBP w 2014 r. – o 35% więcej niż w 2012 r[16].

Sektor prywatny jest zaangażowany w różne działania w ramach obszarów tematycznych przedstawionych na powyższej ilustracji[17].

Strategia cyberbezpieczeństwa Wielkiej Brytanii z 2016 r. także poświęca dużo uwagi współpracy rządu z biznesem w celu wspierania innowacyjnego i dobrze prosperującego sektora cyberbezpieczeństwa[18]. Już dziś Londyn zajmuje szóste miejsce na świecie wśród miast najbardziej sprzyjających startupom. Rząd brytyjski wspiera powstawanie klastrów przedsiębiorstw *high-tech*.

Strategia definiuje sukces w rozwoju sektora prywatnego jako:

- „ponadprzeciętny globalny wzrost brytyjskiego sektora cyberbezpieczeństwa z roku na rok" oraz
- „znaczny wzrost inwestycji w przedsiębiorstwa sektora cyberbezpieczeństwa we wczesnym stadium rozwoju[19]."

Rząd brytyjski wspiera badania podstawowe w 13 Akademickich Centrach Doskonałości Badań Cyberbezpieczeństwa (*Academic Centres of Excellence in Cyber Security Research*) na brytyjskich uniwersytetach[20]. Ponadto rząd zachęca przedsiębiorstwa, aby dołączyły do *CyberInvest* – partnerstwa publiczno-prywatnego, którego celem jest inwestowanie w badania akademickie[21]. Przewidziana wysokość inwestycji wynosi od 10 tys. GBP dla mikroprzedsiębiorstw (poniżej 10 pracowników) do 500 tys. GBP dla dużych przedsiębiorstw (ponad 250

pracowników). 24 spółki zobowiązały się zainwestować minimum 8 mln GBP w ciągu następnych 5 lat w ramach *CyberInvest*[23].

Najnowszym elementem brytyjskiego ekosystemu cyberbezpieczeństwa jest Narodowe Centrum Cyberbezpieczeństwa (*National Cyber Security Centre* – NCSC)[24]. NCSC jest częścią Centrali Łączności Rządowej (*Government Communications Headquarters*) odpowiedzialną za agregację wiedzy i *know-how* w zakresie cyberbezpieczeństwa w celu wsparcia zarówno piodmiotów publicznych, jak i prywatnych w świetle nowego, zintegrowanego podejścia rządu do organizacji brytyjskiego ekosystemu cyberbezpieczeństwa[25]. Do głównych zadań NCSC należy wsparcie dostawców usług kluczowych oraz operatorów infrastruktury krytycznej poprzez wspomaganie wymiany informacji oraz koordynację reakcji na poważne cyberzagrożenia korzystając z wiedzy i podmiotów rządowych, prywatnych oraz społeczności akademickiej. W ramach NCSC działa *Cyber Security Information Sharing Partnership* – partnerstwo na rzecz wymiany informacji stanowiące platformę zrzeszającą właścicieli sieci. NCSC współpracuje także z podmiotami prywatnymi, przeważnie firmami wchodzącymi w skład krajowej infrastruktury krytycznej, w celu dostarczania dedykowanych usług z zakresu cyberbezpieczeństwa[26]. NCSC bierze także udział w programie *CyberFirst*, którego celem jest rozwój i kształcenie następnego pokolenia brytyjskich cyberspecjalistów.

SINGAPUR
NA DRODZE DO „SMART NATION"

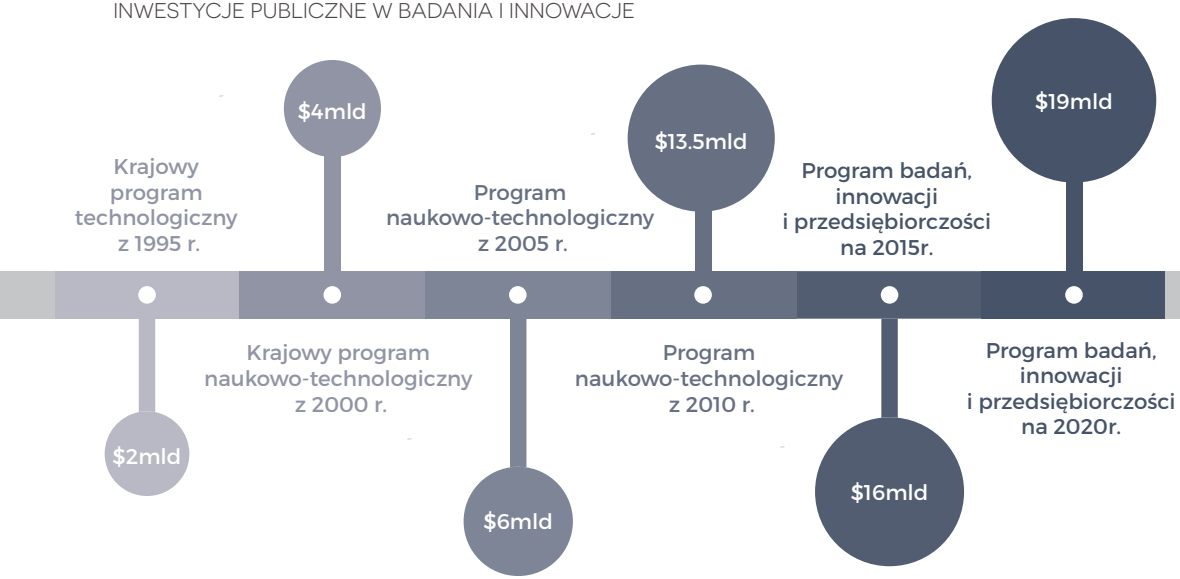
> ***Cyberbezpieczeństwo ma kluczowe znaczenie, jeżeli mamy stać się „smart-nation". Będąc podatnym na cyberzagrożenia nie można korzystać z elektronicznej dokumentacji medycznej, technologii finansowych i wielkich baz danych. (...) Moim zdaniem cyberbezpieczeństwo jest nieodłączną częścią „smart nation".***
>
> — Vivian Balakrishnan, Minister Spraw Zagranicznych oraz minister odpowiedzialny za inicjatywę „Smart Nation"

Singapur jest najbardziej zglobalizowaną gospodarką, która stale zajmuje najwyższe miejsca w kategoriach swobody działalności gospodarczej, otwartości oraz praworządności[27]. Singapurskie wydatki brutto na B+R (GERD) wzrosły z 2,0% PKB w 2013 r. do 2,2% PKB w 2014 r. Ponadto wydatki przedsiębiorstw na prace badawczo-rozwojowe (BERD) wzrosły z 1,2% PKB w 2013 r. do 1,3% PKBw 2014 r.[28]

Singapur zajmuje 10 miejsce na świecie (pierwsze w Azji) w rankingu miast najbardziej sprzyjających startupom[29]. Singapur pragnie stać się zaawansowanym technologicznie krajem (*smart nation*), którego fundamentem jest kompleksowe podejście do cyberbezpieczeństwa.

W kwietniu 2015 r. rząd Singapuru ustanowił Agencję ds. Cyberbezpieczeństwa (*Cyber Security Agency* – CSA). Jest to organ

INWESTYCJE PUBLICZNE W BADANIA I INNOWACJE



usytuowany w ramach Kancelarii Premiera i kierowany przez Ministra Komunikacji i Informacji (*Minister of Communications and Information*). W ciągu pierwszego roku swojego funkcjonowania, CSA przeprowadziła konsultacje z przedstawicielami ponad 50 agencji rządowych, biznesu i samorządów zawodowych oraz instytucji akademickich w zakresie opracowania strategii cyberbezpieczeństwa. W październiku 2016 r. Singapur wprowadził w życie swoją strategię cyberbezpieczeństwa, która opiera się na czterech filarach[30 i 31]:

Budowanie odpornej infrastruktury

w celu wzmocnienia infrastruktury krytycznej w bliskiej współpracy z sektorem prywatnym oraz pozostałymi interesariusami krajowego systemu cyberbezpieczeństwa

Tworzenie bezpieczniejszej cyberprzestrzeni

przez promowanie zaangażowania rządu, przemysłu i ogółu społeczeństwa

Rozwój prężnego ekosystemu cyberbezpieczeństwa

przez współpracę z przemysłem i środowiskiem akademickim w celu powiększenia kadry specjalistów ds. cyberbezpieczeństwa

Zacieśnianie współpracy międzynarodowej

szczególnie pośród członków ASEAN, aby rozwiązywać ponadnarodowe problemy w dziedzinie cyberbezpieczeństwa

Każdy z czterech filarów przewiduje, że sektor prywatny będzie odgrywał kluczową rolę[32]. W ramach Filaru nr 3 (prężny ekosystem cyberbezpieczeństwa) wyraźnie określono zadania rządu na rzecz wsparcia biznesu. Podobnie jak w omówionych powyżej strategiach, rząd inwestuje w prace badawczo-rozwojowe. Singapur rozpoczął 5-letni, wart 130 mln SGD (92,6 mln USD) Narodowy Program Badawczo-Rozwojowy w dziedzinie Cyberbezpieczeństwa (*National Cybersecurity R&D Programme*), aby promować współpracę agencji rządowych, środowiska akademickiego, instytutów badawczych oraz sektora prywatnego[32]. Jest to zaledwie ułamek wartego 19 mld SGD (13,5 mld USD) budżetu Planu Innowacyjności 2020 (*Research Innovation Enterprise 2020 Plan* - RIE2020), którego celem jest wsparcie badań i ich przełożenia na praktyczne rozwiązania odpowiadające na krajowe wyzwania, zwiększenie ilości wdrożeń innowacji technologicznych w przedsiębiorstwach oraz stymulowanie wzrostu gospodarczego przez tworzenie wartości[33]. Około 40% środków możliwe jest do uzyskania na zasadach konkurencji. Program RIE2020 jest ukierunkowany na cztery główne domeny technologiczne, z których każda obejmuje działania na rzecz cyberbezpieczeństwa:

- Zaawansowana produkcja i inżynieria
- Nauki o zdrowiu i biomedycyna
- Usługi i gospodarka cyfrowa
- Rozwiązania urbanistyczne i zrównoważony rozwój[34]

Rozwój przewagi Singapuru w dziedzinie cyberbezpieczeństwa powinien się odbyć przy udziale silnych, lokalnych firm. Budujemy sektor [cyberbezpieczeństwa] poprzez przyciąganie i zatrzymywanie firm o zaawansowanych możliwościach. Będziemy również wspierać startupy, aby przyspieszyć rozwój niszowych i zaawansowanych rozwiązań oraz pomagać rozwijać się lokalnym liderom (...). Będziemy także rozwijać możliwości rynkowe, aby wprowadzać rozwiązania opracowane w Singapurze na rynek globalny.

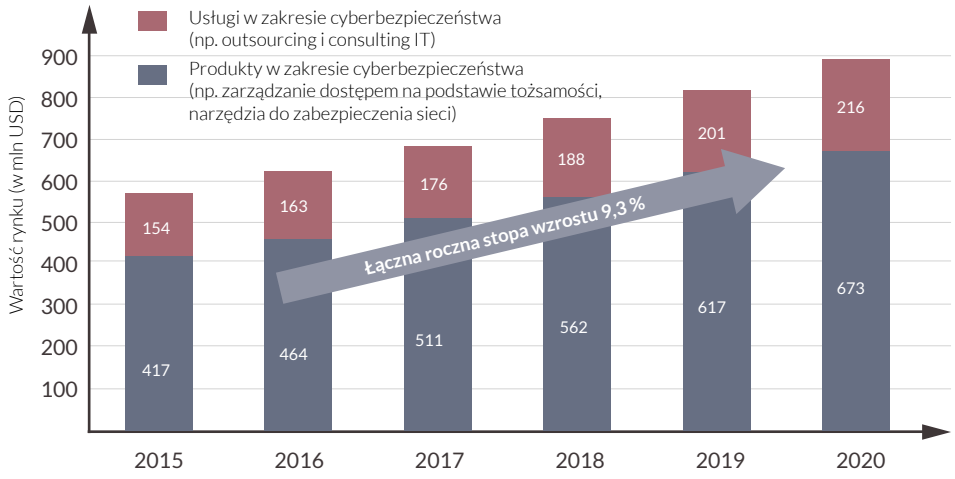
Oficjalne stanowisko rządowe zawarte w Strategii Cyberbezpieczeństwa Singapuru

Przewiduje się, że rynek lokalny będzie rósł w tempie 9% rocznie[35] a globalny rynek cyberbezpieczeństwa będzie wykazywał łączną roczną stopę wzrostu 11,8 %. Oznacza to wzrost od 71 mld USD w 2013 r. do 155 mld USD w 2020 r[36].

CSA rozpoczęła pracę nad inicjatywami, takimi jak Program Partnerstwa i Technologii w zakresie Cyberbezpieczeństwa (*Cyber Security Associates and Technologies* – CSAT), który ma na celu szkolenie i podnoszenie kompetencji specjalistów ICT pod kątem zawodów w dziedzinie cyberbezpieczeństwa oraz program wprowadzenia certyfikacji CREST. CSA podpisała również porozumienia z Politechniką Nanyang (*Nanyang Polytechnic*) oraz Singapurskim Instytutem Technologicznym (*Singapore Institute of Technology*) w celu rozwoju narodowych kompetencji w zakresie cyberbezpieczeństwa.

Ponadto, rząd Singapuru postanowił rozwijać przemysł lokalny. Powyższy cytat jest szczególnie ważny w tym kontekście. Singapur słynie z aktywnego poszukiwania najlepszych praktyk na całym świecie w celu rozwiązywania swoich problemów i wykorzystywania nadarzających się szans rynkowych. Strategia

SZACOWANY WZROST SINGAPURSKIEGO RYNKU CYBERBEZPIECZEŃSTWA W LATACH 2015–2020[37]



Singapuru pokazuje, że podejście wybrane lata temu przez Izrael i Wielką Brytanię polegające na rozwoju innowacji, szczególnie poprzez pomoc publiczną dla przedsiębiorstw w dziedzinie cyberbezpieczeństwa jest rzeczywiście skuteczne. W Singapurze obecni są wszyscy istotni interesariusze: międzynarodowe korporacje finansowe, jednostki badawczo-rozwojowe m.in. Boeing, NEC czy INTERPOLu[38]. Singapurski rząd może pozwolić sobie na zakup dowolnego, dostępnego na rynku rozwiązania i przez lata realizował właśnie takie, tradycyjne podejście do cyberbezpieczeństwa. Teraz postanowił iść w ślad za Wielką Brytanią i Izraelem: zwiększyć lokalny poziom działań badawczo-rozwojowych i wesprzeć sektor cyberbezpieczeństwa. Singapur to najbardziej wolnorynkowa gospodarka na świecie oferująca wyjątkowo równe warunki prowadzenia działalności gospodarczej i otwarte środowisko biznesowe. Tym niemniej Singapur wiąże swoje ambicje z rynkiem globalnym, a nie tylko konsumpcją krajową. To podejście strategiczne obala argumenty ideologiczne, które często są podnoszone przeciwko istotnemu wsparciu krajowego sektora biznesowego przez rząd.

WNIOSKI
RZĄDY WIODĄCYCH KRAJÓW W DZIEDZINIE CYBERBEZPIECZEŃSTWA WSPIERAJĄ BIZNES W TWORZENIU I WDRAŻANIU INNOWACJI

Wszystkie trzy przeanalizowane krajowe strategie cyberbezpieczeństwa cechują się uderzająco podobnym podejściem do poprawy współpracy administracji z biznesem w celu tworzenia i wdrażania innowacji w sektorze cyberbezpieczeństwa. Zarówno Wielka Brytania, jak i Izrael oraz Singapur zainwestowały znaczne środki publiczne w celu utworzenia akademickich centrów doskonałości na rzecz radykalnych innowacji i gruntownych zmian obecnych praktyk i procesów.

Często stosowane jest regionalne skupienie kompetencji. Izrael utworzył główny klaster ICT w okolicy Tel Awiwu oraz rozwija nowy klaster cyberbezpieczeństwa w Beer Szewie. Pojawienie się m.in. „Ronda Krzemowego" w Londynie oraz „Cyberdoliny" w Malvern przypomina nieco działania Izraela w Beer Szewie. Singapurskie Biopolis na rzecz rozwoju nauk biomedycznych należy do najbardziej ambitnych spośród tego rodzaju projektów.

Bezpośrednie wsparcie rządowe dla przedsiębiorstw obejmuje:

- Zapewnianie grantów na prace badawczo-rozwojowe
- Zlecanie działań badawczo-rozwojowych firmom komercyjnym
- Generowanie popytu krajowego
- Pomoc w dostępie do rynków zagranicznych
- Udzielanie zasobów rządowych przedsiębiorstwom w celach badawczo-rozwojowych[39]

Pośrednie wsparcie rządowe dla całego Narodowego Systemu Innowacji obejmuje:

- Wsparcie fiskalne oraz inne zachęty dla niekomercyjnych instytucji badawczych
- Wsparcie prawno-finansowe dla współpracy środowiska akademickiego z biznesem w wybranych tematach (mechanizmy transferu technologii)
- Zachęty podatkowe dla wydatków na badania i rozwój w sektorze prywatnym
- Infrastrukturę umożliwiającą wspólną lokalizację (*colocation*).

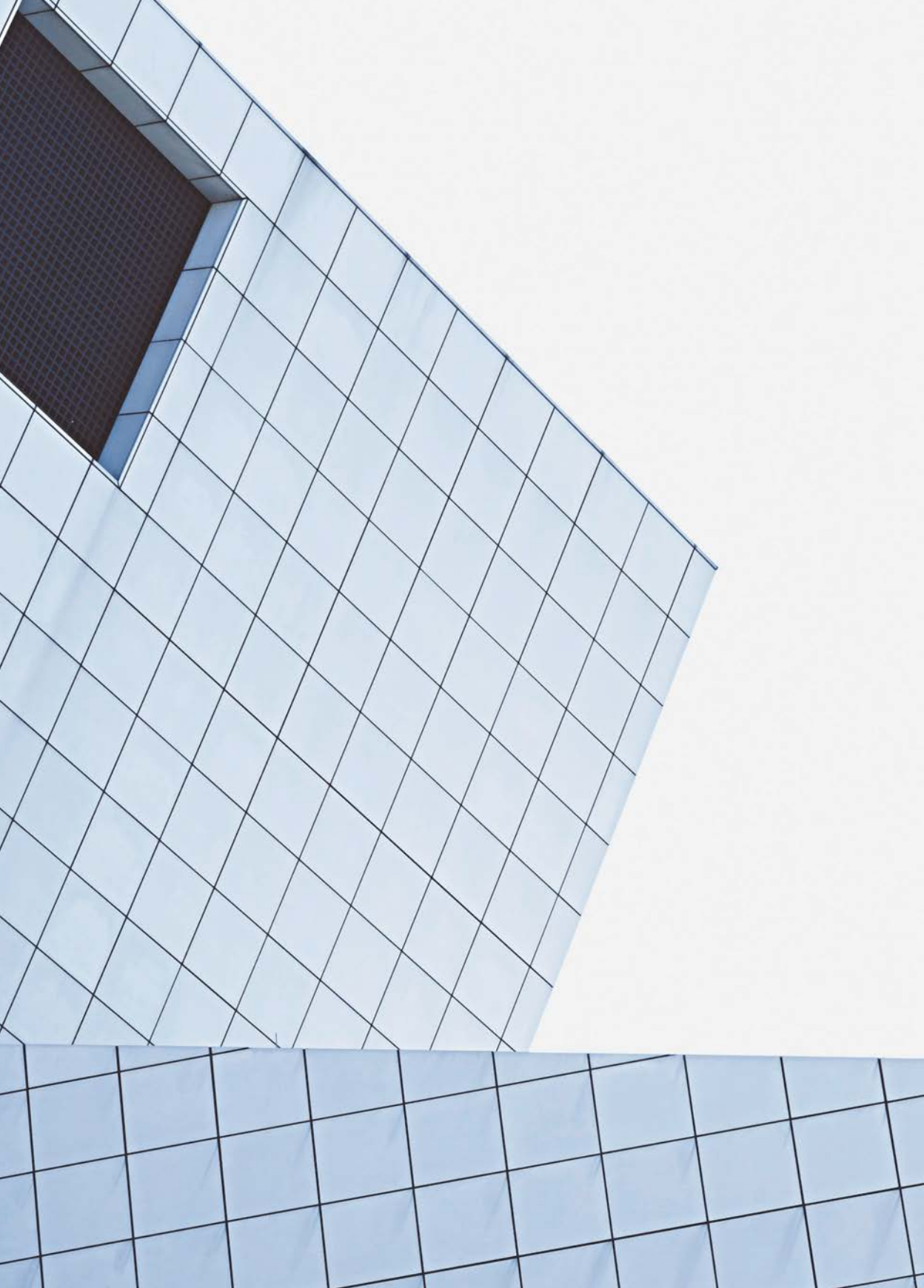
TA KRÓTKA ANALIZA PROWADZI DO NASTĘPUJĄCYCH WNIOSKÓW:

- Innowacyjność znacznie przyczynia się do cyberbezpieczeństwa. To nie zbieg okoliczności, że wiodące światowe cyberpotęgi są także wiodącymi innowatorami.
- Sukces innowacji w dużym stopniu zależy od strategii i polityki rządu. Wszystkie trzy przeanalizowane krajowe strategie cyberbezpieczeństwa dążą do innowacji na rzecz cyberbezpieczeństwa.
- Od 2011 r. Izrael i Wielka Brytania przygotowały serię rządowych dokumentów i poświęciły specjalnie przeznaczone na ten cel zasoby aby wesprzeć współpracę administracji z biznesem. Te działania wytworzyły rzeczywistą wartość gospodarczą oraz rozwój w dziedzinie bezpieczeństwa.
- Teraz Singapur przyjął takie podejście stawiając m.in. na znaczną rozbudowę lokalnego przemysłu.

SOURCES:

1. Organizacja Współpracy Gospodarczej i Rozwoju, Podręcznik Frascati z 2015 r.: *Wytyczne OECD w zakresie zbierania i raportowania danych dotyczących badań i rozwoju eksperymentalnego* (Paryż: OECD, 2015).
2. Tabansky, L. and I. Ben Israel (2015). *The National Innovation Ecosystem of Israel. Cybersecurity in Israel*, Springer International Publishing: 15-30.
3. OECD estimates based on OECD Main Science and Technology Indicators Database, February 2017, www.oecd.org/sti/inno/rd_intensities.xls.
4. https://www.bloomberg.com/graphics/2015-innovative-countries/.
5. Financial Times, https://www.ft.com/content/dfa5c916-b90e-11e5-b151-8e15c9a029fb.
6. http://www.pmo.gov.il/English/MediaCenter/Spokesman/Pages/spokeCyber150215.aspx.
7. *Israel's Computer-Security Firms: Cyber-Boom or Cyber-Bubble?*, Economist 411, nr 8945 (2015).
8. *The Global Startup Ecosystem Report 2015*, https://ec.europa.eu/futurium/en/system/files/ged/the_global_startup_ecosystem_report_2015_v1.2.pdf.
9. The Supreme Council on Science and Technology, *The National Cyber Initiative – a Special Report for the Prime Minister* (Jerusalem: Ministry of Science and Technology National Council on Research and Development, 2011).
10. Israel, G. o. (2011). Government decision 3611: *Promoting national capacity in cyber space*, Jerusalem, Israel, PMO Secretariat.
11. http://cyberspark.org.il/why-beer-sheva/ (access: 11/05/2017).
12. HM Government, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, Cabinet Office, http://www.cabinetoffice.gov.uk/sites/default/files/resources/uk-cyber-security-strategy-final.pdf.
13. HM Government, *The UK Cyber Security Strategy 2011-2016: final report*.
14. HM Government, *The UK Cyber Security Strategy 2011-2016: final report*.
15. HM Government, *The UK Cyber Security Strategy 2011-2016: final report*.
16. HM Government, *The UK Cyber Security Strategy 2011-2016: final report*.
17. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf.
18. HM Government, *National Cyber Security Strategy 2016-2021*, (UK: HM Government, 2016).
19. HM Government, *National Cyber Security Strategy 2016-2021*.
20. https://www.epsrc.ac.uk/research/centres/acecybersecurity/.
21. Objective 7.3.9. HM Government, *National Cyber Security Strategy 2016-2021*.
22. https://www.ncsc.gov.uk/articles/cyber-invest.
23. https://www.ncsc.gov.uk/articles/cyber-invest.
24. *Britain to enter new era of online opportunity*, https://www.ncsc.gov.uk/news/britain-enter-new-era-online-opportunity (access: 23/05/2017).
25. NCSC consolidates the expertise of the previously existing: CESG (the information security arm of GCHQ), the Centre for Cyber Assessment (CCA), Computer Emergency Response Team UK (CERT UK) and the cyber-related divisions of the Centre for the Protection of National Infrastructure
26. An overview of the National Cyber Security Centre, https://www.ncsc.gov.uk/document/ncsc-overview, (access: 23/05/2017).

27. https://www.weforum.org/agenda/2016/11/top-10-global-enabling-trade-report-2016/ http://www.heritage.org/index/country/singapore.
28. Agency for Science, Technology and Research (A*STAR), Annual Report 2014 – 2015 https://www.a-star.edu.sg/Portals/81/Data/News%20And%20Events/Publications/Astar%20Yearbook/Files/Astar%20Yearbook/AStar%20Yearbook/ASTAR%20Annual%20Report_1415.pdf.
29. *The Global Startup Ecosystem Report 2015*, https://ec.europa.eu/futurium/en/system/files/ged/the_global_startup_ecosystem_report_2015_v1.2.pdf.
30. Cyber Security Agency of Singapore, *Singapore's Cybersecurity Strategy*, (Singapore 2016).
31. Own elaboration based on the official strategy document.
32. https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme (access: 11/05/2017).
33. http://www.channelnewsasia.com/news/business/govt-commits-s-19b-to-new-5-year-plan-for-r-amp-d-initiatives-ri-8214052 (access: 11/05/2017).
34. https://www.nrf.gov.sg/rie2020 (access: 11/05/2017).
35. https://www.forbes.com/sites/stevemorgan/2015/12/20/cybersecurity%E2%80%8B-%E2%80%8Bmarket-reaches-75-billion-in-2015%E2%80%8B%E2%80%8B-%E2%80%8Bexpected-to-reach-170-billion-by-2020/ (access: 11/05/2017).
36. Frost & Sullivan Global, Cybersecurity Market Assessment, 2014.
37. https://www.slideshare.net/benjaminang/singapores-nationalcyber-security-strategy, 2017 (access: 11/05/2017).
38. http://www.startupdecisions.com.sg/blog/edb-promotes-cyber-security-singapore/.
39. Think U.S. defense mega-contractors and U.S. defense and intelligence agencies.



NOWOCZESNY I INNOWACYJNY SEKTOR ICT: KLUCZOWA CZĘŚĆ KRAJOWEGO EKOSYSTEMU CYBERBEZPIECZEŃSTWA

ROBERT SIUDAK

Rosnące znaczenie Internetu w gospodarce, rewolucja w sprawach wojskowych oraz zmieniające się wskutek rozwoju nowych mediów wzorce informacyjne stwarzają nowe wyzwania dla krajowych strategii zarówno w sektorze wojskowym, jak i cywilnym. Cyberprzestrzeń stała się „układem nerwowym" nowoczesnego społeczeństwa informacyjnego[1], stając się kolejnym, obok lądu, morza i powietrza, obszarem działania państwa. O unikalnym charakterze tego obszaru świadczą jego elementy składowe:

- sprzęt („hardware" – warstwa fizyczna);
- oprogramowanie („software") i protokoły (warstwa syntaktyczna/logiczna);
- informacje (warstwa semantyczna)[2].

Jego dwa pierwsze komponenty są efektem działalności podmiotów prywatnych operujących na otwartym rynku. Ten prosty fakt techniczny należy uznać za podstawową przyczynę daleko idących konsekwencji politycznych, z których najważniejszą jest to, że bez rozbudowanego i zaawansowanego krajowego sektora ICT, zdolności państwa w zakresie cyberbezpieczeństwa są bardzo ograniczone.

Wspólny mianownik – ICT, cyberbezpieczeństwo, innowacje

Dojrzały sektor ICT należy postrzegać jako siłę napędową zarówno krajowego cyberbezpieczeństwa, jak i innowacyjności. Nieprzypadkowo podobna grupa państw znajduje się równocześnie na liście *Fortune 500 Global Rank* w dziedzinie technologii oraz *Global Cybersecurity Index & Cyberwellness* w dziedzinie cyberbezpieczeństwa. W ostatnim wydaniu rankingu Forbes z 2016 r. znalazły się 33 firmy technologiczne, zaś wiodącym krajem są Stany Zjednoczone

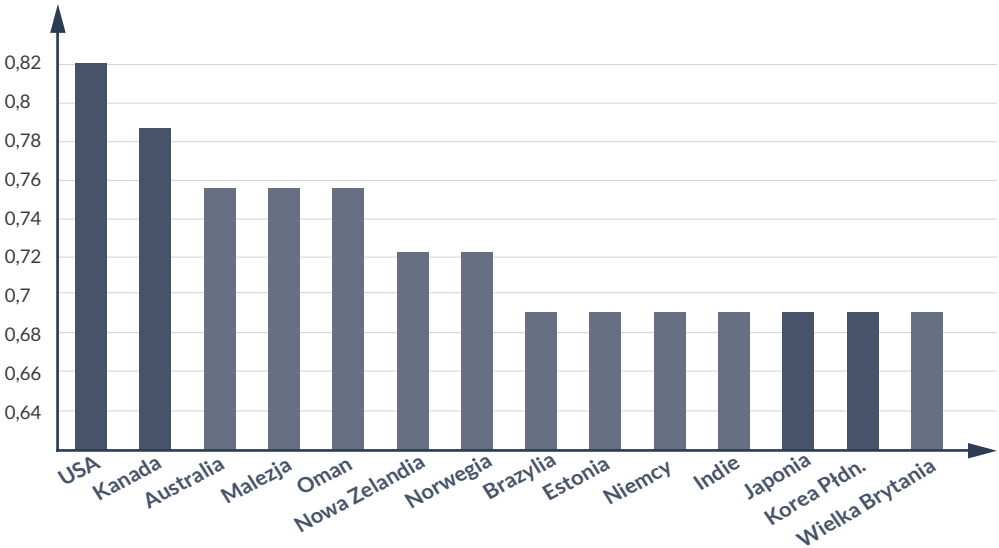
RANKING FORBES GLOBAL 500, TECHNOLOGIA – FIRMY Z PODZIAŁEM NA PAŃSTWA

Źródło: Fortune, Global 500,sektor technologiczny, 2016 r.

z 11 przedstawicielami. Na kolejnych miejscach uplasowały się: Japonia i Tajwan z 5, Chiny z 4 oraz Korea Południowa z 3[3]. Dla porównania, ostatni ranking *Global Cybersecurity Index & Cyberwellness* opublikowany przez Międzynarodowy Związek Telekomunikacyjny (*International Telecommunication Union* – ITU) oraz ABI Research w 2015 r., określa USA jako lidera. Japonia i Korea Południowa zajmują 5 miejsce, zaś Chiny 14[4]. Polska uplasowała sią na 11 miejscu na liście ITU ze wskaźnikiem 0,592.

Sektor prywatny jest głównym źródłem rozwiązań w dziedzinie technologii (ICT) na współczesnym rynku. Głównej przyczyny takiego stanu rzeczy należy upatrywać w strukturze współczesnej gospodarki.

RANKING GLOBAL CYBERSECURITY INDEX & CYBERWELLNESS

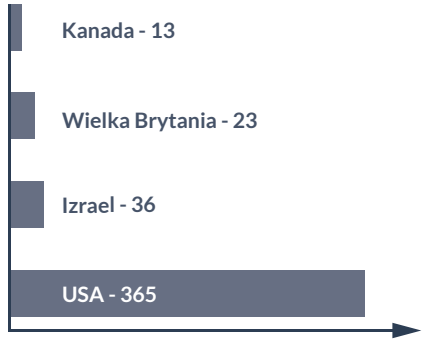


Międzynarodowy Związek Telekomunikacyjny (ITU), Global Cybersecurity Index & Cyberwellness Profiles, 2015 r.

Jak omówiono w poprzednim rozdziale, sektor prywatny czerpie korzyści z połączonych badań podstawowych i stosowanych, przekształcając je w rozwój nowych produktów i usług. Ze względu na fakt, iż potrzeby rynkowe stanowią katalizator innowacji w gospodarce cyfrowej, nie jest niespodzianką, że sekcja zaawansowanych technologii rankingu *Bloomberg Innovation Index* z 2015 r. obejmuje tę samą grupę państw, co *Forbes 500 Global* omówiony powyżej: USA (miejsce 1), Chiny (2), Japonię (3), Koreę Południową (4) i Kanadę (5)[5].

W jaki sposób wszystko to wpływa na bezpieczeństwo cyberprzestrzeni? Według raportu Symantec codziennie powstaje około milion nowych złośliwych programów (malware)[6]. Hackmageddon, który monitoruje większe ataki sieciowe, szacuje ilość zdarzeń w 2016 r. na 1061, co daje ponad 3 ataki na dużą skalę dziennie[7]. Z uwagi na szybko zmieniające się środowisko zagrożeń, sektor cyberbezpieczeństwa stanowi jeden z najdynamiczniej ewoluujących obszarów ICT. Aby sprostać zagrożeniom, firmy oferujące produkty oraz usługi dla cyberbezpieczeństwa muszą być innowacyjne. Analiza rankingu *Cybersecurity 500*, który obejmuje najbardziej innowacyjne przedsiębiorstwa w zakresie cyberbezpieczeństwa na świecie, potwierdza, że istnieją dwa kluczowe wskaźniki pozwalające na stworzenie prężnego krajowego ekosystemu cyberinnowacji[8]. Pierwszym z nich jest dojrzały i konkurencyjny na arenie międzynarodowej sektor ICT, drugim istnienie Narodowego Systemu Innowacji, omówionego w poprzednim rozdziale. Pierwsze trzy kraje z najwyższą liczbą przedstawicieli na liście *Cybersecurity 500* w 2017 r. posiadają jedno i drugie: USA z 365 firmami, Izrael z 36 oraz Wielka Brytania z 23 przedstawicielami.

RANKING CYBERSECURITY 500 – FIRMY Z PODZIAŁEM NA PAŃSTWA



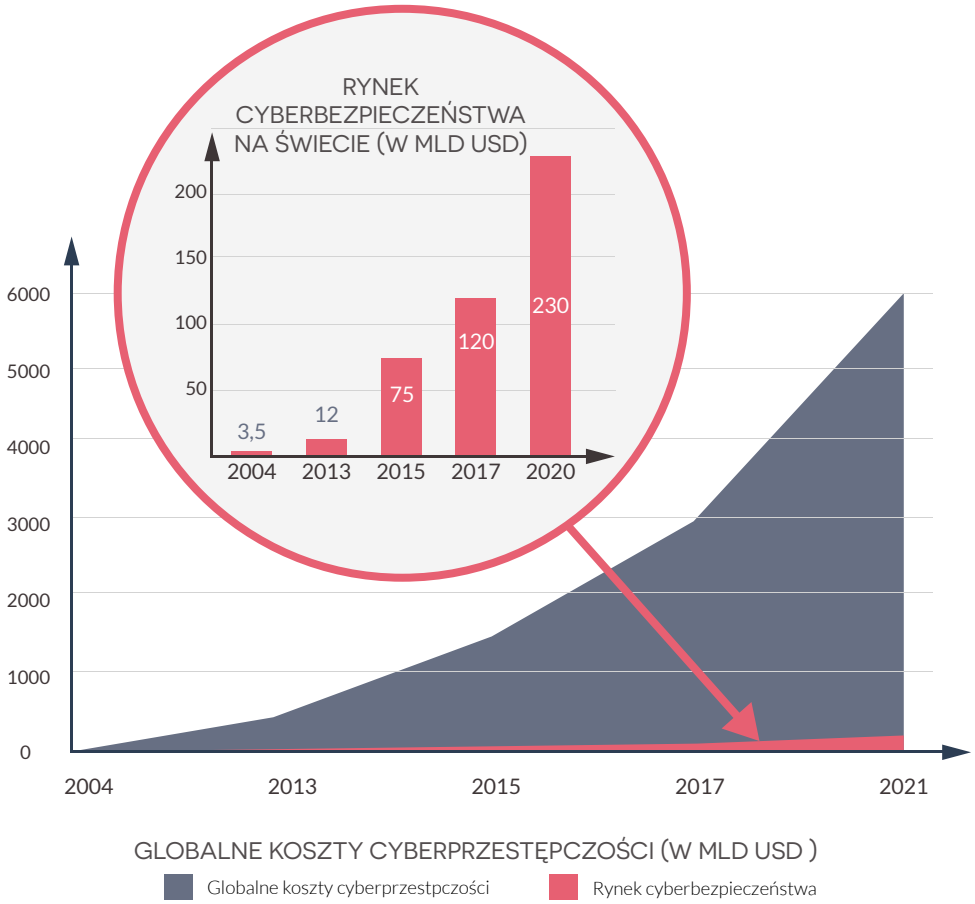
Źródło: Cybersecurity Ventures, The Cybersecurity 500, 2017 r.

Cyberbezpieczeństwo jako przewaga konkurencyjna

Stopniowo stajemy się bardziej świadomi tego, jak wrażliwe, a zarazem niezbędne, są nasze sieci i systemy. Wiele raportów sugeruje, że rok 2016 był przełomowy pod kątem publicznego postrzegania cyberbezpieczeństwa[9]. Przestało ono być odległym problemem technicznym, istotnym tylko dla działów informatycznych, a stało się integralną częścią strategii firm, operacji finansowych i życia prywatnego. Zdaliśmy sobie sprawę, że cyberbezpieczeństwo będzie jednym z zasadniczych wyzwań przez

najbliższe dekady. Jednak to wyzwanie równocześnie stanowi wielką szansę dla tych, którzy będą potrafili ją wykorzystać.

Cyberbezpieczeństwo stanowi jeden z najszybciej rozwijających się sektorów rynku ICT. W 2017 r. światowe wydatki na produkty i usługi związane z cyberbezpieczeństwem wyniosą ponad 120 miliardów USD[10]. W ostatniej dekadzie byliśmy świadkami rozwoju tego rynku w tempie 8–10% rocznie, a prognozy na lata 2017–2020 wskazują dalszy stabilny wzrost do łącznej, skumulowanej sumy 1 biliona USD. Szacuje się, że w latach 2015–2020 łączna wartość produktów i usług mających



Źródło: Opracowanie własne w oparciu o raporty Gartner, Visiongain, Cybersecurity Ventures, Markets and Markets
Źródło: Cybersecurity Ventures, 2016 Cybercrime Report, 2016 r.

na celu samo zabezpieczenie Internetu Rzeczy (*Internet of Things* – IoT) osiągnie aż 120 mld USD, czyli obecną wartość całego rynku cyberbezpieczeństwa[11].

Specyfika sytuacji polega na fakcie, że rozwój sektora cyberbezpieczeństwa napędzany jest głównie przez skalę zagrożeń rosnących w tempie wykładniczym, zaś w mniejszym stopniu przez przełomowe technologie czy optymalizację procesów. Trudno jest określić całkowite straty sektora publicznego i prywatnego wynikające z cyberprzestępczości, jednak szacuje się, że obecnie wynoszą one około 1% światowego PKB[12]. Ponadto badacze przewidują, że do 2021 r. straty te będą wynosić ponad 6 bilionów USD rocznie[13]. Mamy zatem do czynienia z szybko rozwijającym się rynkiem napędzanym przez inherentną podatność ICT.

Silny rynek cyberbezpieczeństwa może nie tylko stać się dochodową niszą dla krajowych firm z branży ICT, jak ma to miejsce w Izraelu i Wielkiej Brytanii, ale powinien także przynosić długoterminowe korzyści dla całej gospodarki, zapewniając łatwo dostępne produkty i usługi dla sektora prywatnego i publicznego. To z kolei pozwoli poprawić wskaźniki makroekonomiczne gospodarki. Standard and Poor's wydało w 2015 r. oświadczenie o obniżeniu ocen dla kredytodawców, którzy nie bronią się skutecznie przed cyberatakami, co tylko potwierdzają tę zależność[14]. Wreszcie, dojrzały krajowy rynek zapewniający światowej klasy rozwiązania w zakresie ochrony infrastruktury ICT należy postrzegać jako bazę techniczną i czynnik umożliwiający prowadzenie przez rządy zaawansowanej polityki w zakresie cyberbezpieczeństwa.

Trudno jest określić całkowite straty sektora publicznego i prywatnego na świecie wynikające z cyberprzestępczości, jednak szacuje się, że obecnie wynoszą one około 1% światowego PKB.

Budowanie cybersuwerenności

Korzyści, jakie przynosi dla rynku inteligentna specjalizacja w zakresie cyberbezpieczeństwa to tylko jedna strona równania. Drugą jest koncepcja cybersuwerenności, u podstaw której leży założenie, że infrastruktura ICT posiada narodowość, co z kolei pociąga za sobą istotne konsekwencje dla cyberbezpieczeństwa. Aby móc chronić własną cyberprzestrzeń i podejmować suwerenne decyzje polityczne na współczesnej arenie międzynarodowej, państwo musi mieć do dyspozycji konkurencyjny, krajowy sektor ICT. Zdolność nabywania kodów źródłowych, rozwijania najnowocześniejszych, dedykowanych produktów i usług, a także możliwość współpracy z producentem w celu monitorowania

procesów wdrażania technologii na zamówienie w ramach inteligentnych usług stanowi konieczność w wypadku wielu krytycznych systemów. Dobrym przykładem tego problemu jest chiński zakaz stosowania systemu operacyjnego Windows 8 z powodów bezpieczeństwa[15], czy też wykluczenie Huawei z udziału w przetargach na kontrakty dla rządu USA z obawy o szpiegostwo[16].

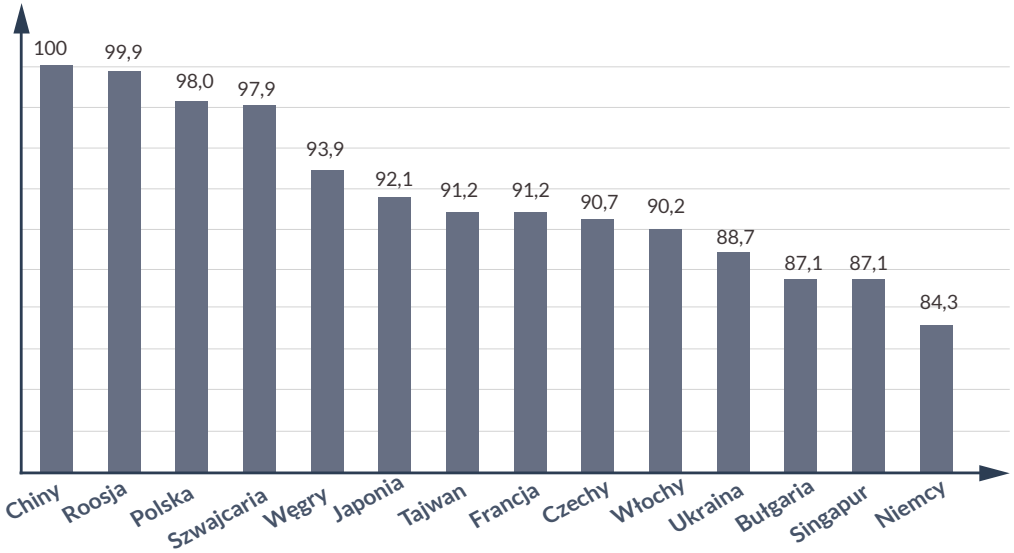
Ważne jest, aby postrzegać krajowy sektor ICT nie tylko jako dostawcę produktów i usług na rynku, ale jako istotną część całego ekosystemu cyberbezpieczeństwa opartego na czterech głównych elementach wytwarzanych w ramach współpracy sektora prywatnego i publicznego:

- krajowe kadry w dziedzinie cyberbezpieczeństwa z odpowiednią wiedzą ekspercką;
- sprzęt i infrastruktura zapewnione przez krajowych producentów ICT;
- oprogramowanie i komponenty logiczne (protokoły i normy) stworzone, utrzymywane i obsługiwane przez firmy krajowe;
- ogólnokrajowy system cyberbezpieczeństwa stanowiący zachętę dla współpracy interesariuszy prywatnych i publicznych oraz wprowadzający innowacyjne rozwiązania.

Oprócz omówionej już roli krajowego rynku ICT związanej z podażą, reprezentowaną przez elementy 2 i 3 oraz roli systemowej odzwierciedlonej w elemencie 4, sektor prywatny musi brać aktywny udział w edukowaniu i szkoleniu krajowych kadr związanych z cyberbezpieczeństwem. Zapotrzebowanie na specjalistów cyberbezpieczeństwa wzrasta w tempie wykładniczym i przewiduje się, że na całym świecie do 2019 r. będzie 6 milionów miejsc pracy w tym sektorze oraz 1,5 miliona wakatów[17]. Zinstytucjonalizowane szkolnictwo nie nadąża za szybko ewoluującym obszarem cyberbezpieczeństwa, co stwarza potrzebę zaangażowania przedsiębiorstw poprzez wykorzystanie ich fachowej wiedzy i doświadczenia.

Wiele państw już zrozumiało strategiczną rolę krajowego sektora ICT w dążeniu do zapewnienia bezpiecznej cyberprzestrzeni. Jak przedstawiono w poprzednim rozdziale Izrael, Wielka Brytania i Singapur już wprowadziły dedykowane programy wsparcia krajowych innowacji w dziedzinie cyberbezpieczeństwa. Inne kraje, takie jak USA, Chiny, Korea Południowa i Japonia także aktywnie wspierają swój przemysł cyfrowy. Unia Europejska uznała, że w obliczu faktu, iż „światowy rynek cyberbezpieczeństwa jest zdominowany przez globalnych dostawców z Ameryki Północnej”[18], Europa musi zacząć odgrywać bardziej aktywną rolę. Jak wyszczególniono w pierwszym rozdziale niniejszego raportu, w 2016 r. Komisja Europejska wraz z Europejską Organizacją na rzecz Cyberbezpieczeństwa (ECSO) podpisały umowę o partnerstwie publiczno-prywatnym (PPP), której celem jest rozwój konkurencyjnego rynku europejskiego przez zainicjowanie do 2020 r. inwestycji wartych 1,8 mld EUR.

KRAJE Z NAJLEPSZYMI PROGRAMISTAMI – HACKER RANK INDEX



Źródło: HackerRank, Which Country Would Win in the Programming Olympics?, 2017 r.

Polska – niewykorzystany potencjał

W 2016 r. polski rynek ICT wart był około 8,5 mld USD[19]. Jest to wynik stałego wzrostu na średnim rocznym poziomie 5-6% w ostatnich dwóch dekadach. Transformacja polskiej gospodarki w ostatnich 28 latach spowodowała ogromną zmianę w postaci odejścia od tradycyjnych sektorów, takich jak górnictwo czy metalurgia, na rzecz rozwoju opartego na usługach z rosnącym udziałem technologii informatycznych[20]. Firmy z branży ICT, które w tym czasie zdobyły fachową wiedzę mają niepowtarzalną szansę stanąć na czele cyfrowej transformacji polskiej gospodarki. Głównym zasobem, który rozwinięto w tym czasie i który można wykorzystać w budowie krajowego ekosystemu cyberbezpieczeństwa, są ludzie. Polska obfituje w talenty w zakresie cyberbezpieczeństwa, co potwierdzają liczne rankingi i „hackatony". Polscy programiści i hakerzy wygrywają w prawie wszystkich znanych konkursach informatycznych od Locked Shields (2014 r.), przez cykl Capture the Flag (2014 r.) po nieoficjalne mistrzostwa świata dla programistów, czyli Hello World Open (2014 r.) i Google Code Jam (2012 r.).

Według HackerRank, polscy programiści plasują się na trzecim miejscu, zaraz po informatykach z Chin oraz Rosji. Jeżeli chodzi o język programowania Java, Polska jest na szczycie listy[21]. Co więcej Polska ustępuje tylko Singapurowi wśród wiodących centrów programistycznych z punktu widzenia przedsiębiorstw oraz

inwestorów[22], a to z kolei zwiększa zapotrzebowanie na wykwalifikowanych specjalistów ICT na rynku krajowym. Obecne szacunki wykazują, że w Polskim sektorze ICT wciąż pozostaje 40 000 nieobsadzonych posad, mimo że polskie uczelnie edukują 30 000 nowych absolwentów kierunków związanych z tą branżą każdego roku[23].

Czerpiąc ze światowej klasy zasobów ludzkich, ICT jest jednym z najbardziej konkurencyjnych na świecie sektorów polskiej gospodarki. Od startupów, przez średnie firmy, aż po wielkie przedsiębiorstwa, Polska jest siedzibą dziesiątek rozwijających się na świecie marek. Wiele z nich to liderzy w swoim segmencie rynkowym, a ich działy badawczo-rozwojowe są źródłem wyjątkowych, najnowocześniejszych rozwiązań technologicznych. Inne, dzięki innowacyjnemu modelowi biznesowemu, są w stanie konkurować z największymi globalnymi graczami z Doliny Krzemowej czy Shenzhen.

Jednak światowej klasy kapitał ludzki i otwarte środowisko biznesowe nie wystarczą, aby ekosystem cyberbezpieczeństwa w pełni rozkwitł. Jak postuluje pierwszy rozdział niniejszego raportu, zachodzi potrzeba usprawnienia mechanizmu partnerstwa publiczno-prywatnego, który powinien korzystać z dostępnych zasobów rynkowych i rządowych do wzmocnienia cyberbezpieczeństwa w kraju. Taka międzysektorowa współpraca to również główne wymaganie dla rozwoju polskiego sektora ICT.

Według różnych raportów w ostatnich latach polski rynek ICT zmagał się z dwiema głównymi przeszkodami:

- **Niewystarczającym finansowaniem, zarówno zewnętrznym jak i wewnętrznym, łącznie z kapitałem wysokiego ryzyka. Przedsiębiorstwa uważają ten czynnik za „największą przeszkodę w innowacji"[24].**
- **Małe zapotrzebowanie ze strony sektora publicznego, w tym władz centralnych i lokalnych, jak również przedsiębiorstw państwowych[25].**

Pierwszy z wymienionych problemów szczególnie dotyka startupów sektora cyberbezpieczeństwa i zaawansowanych technologii. Aby odpowiednio rozpowszechnić swoje produkty i wprowadzić ofertę na rynek międzynarodowy potrzebują dostępu do kapitału wysokiego ryzyka. W wielu przypadkach to sama rzeczywistość rynkowa zmusza polskie startupy do poszukiwania inwestorów wśród amerykańskich, francuskich

lub brytyjskich funduszy *venture capital* (VC). Waga drugiego problemu wynika z faktu, że w ostatnim roku wydatki publiczne w Polsce stanowiły 42,1% łącznego PKB[26]. Ta liczba ukazuje wyłącznie wydatki władz centralnych i lokalnych z wyłączeniem spółek skarbu państwa, które zajmują pierwsze 13 miejsc na liście największych firm z polskim kapitałem[27]. Według ankiety przeprowadzonej przez Instytut Kościuszki i Fundację Bezpieczna Cyberprzestrzeń w 2017 r. wśród polskich firm z sektora cyberbezpieczeństwa, 88,9% uznało ograniczony popyt na innowacyjne produkty za główną wadę krajowego rynku cyberbezpieczeństwa. Strategiczne znaczenie obydwu wyzwań potwierdza fakt, że wdrożono już pewne inicjatywy publiczne w celu ich rozwiązania.

Rynek VC powoli rozwija się w Polsce, częściowo dzięki programom rządowym takim jak *Bridge Alfa* czy *Starter*. Łączą one kapitał prywatny z publicznym, co pozwala na tworzenie nowych krajowych funduszy VC. Obydwa projekty stanowią część szerszego programu wsparcia rządowego dla sektora startupów pod hasłem *Start In Poland*, powstają także nowe inicjatywy w przedsiębiorstwach państwowych, z których wiele planuje otwarcie korporacyjnych funduszy *venture capital* (CVC)[28]. Inne, takie jak „fundusz funduszy" Witelo, zaprojektowany w celu inwestowania publicznych środków w polskie startupy za pośrednictwem międzynarodowych funduszy VC, już podpisały umowy z partnerami takimi jak Atomico, Evolution Equity oraz DN Capital[29].

Potrzebne są także systemowe rozwiązania, pomagające w dopasowaniu popytu z sektora publicznego do rynku krajowych produktów i usług w dziedzinie cyberbezpieczeństwa. W tym celu należy utworzyć platformy otwartej współpracy na poziomie centralnym i lokalnym. Cyberpark Enigma zaproponowany w ramach rządowego „Planu na rzecz Odpowiedzialnego Rozwoju" może stać się głównym punktem węzłowym w procesie wzajemnego dostosowania potrzeb publicznych i oferty rynku krajowego[30]. Celem jest przyciągnięcie prywatnych przedsiębiorstw, sektora publicznego a także akademickich ośrodków badawczych do współpracy na wszystkich poziomach łańcucha dostaw. Ponadto lokalne inicjatywy, takie jak Cybersec Hub w Krakowie, który łączy środowisko akademickie, wielkie przedsiębiorstwa i startupy z władzami lokalnymi oraz innymi partnerami publicznymi, stanowią praktyczny przykład regionalnych systemów cyberbezpieczeństwa[31]. Zarówno te, jak i inne propozycje systemowe, np. w postaci specjalnie zaprojektowanego akceleratora startupów, dyskutowane były w trakcie Polskiego Forum Cyberbezpieczeństwa – CYBERSEC PL 2017.

Chociaż pewne inicjatywy zostały już zainicjowane, zachodzi potrzeba podjęcia kluczowych decyzji strategicznych w celu wykorzystania możliwości wynikających z rosnącego rynku cyberbezpieczeństwa.

Wymienione wyżej inicjatywy umożliwią wykorzystanie już powstających technologii

i posiadanych zasobów ludzkich oraz przekształcenie ich w krajowy ekosystem cyberbezpieczeństwa. Ponadto inteligentna specjalizacja w zakresie technologii cyberbezpieczeństwa może stanowić przewagę konkurencyjną całego polskiego sektora ICT. To z kolei wzmocniłoby krajową gospodarkę przez zmianę pozycji Polski w światowym łańcuchu dostaw dla branży ICT. Polska, znana dotychczas z outsourcingu prostych usług, mogłaby stać się ośrodkiem powstawania najnowocześniejszych, innowacyjnych produktów związanych z cyberbezpieczeństwem.

Aby stać się jednym z centrów kompetencji oraz ośrodkiem tworzącym światowej klasy produkty w dziedzinie cybertechnologii, należy podjąć co najmniej sześć pierwszych kroków:

- Ustanowić ogólnokrajowe partnerstwo publiczno-prywatne w zakresie cyberbezpieczeństwa, aby wesprzeć inwestycje na rynku wewnętrznym;
- Uruchomić serię programów badawczo-rozwojowych w dziedzinie cyberbezpieczeństwa, aby zachęcić środowisko akademickie do prowadzenia badań podstawowych i stosowanych w tej dziedzinie;
- Stworzyć zachęty dla przedsiębiorców w celu rozszerzenia ich inwestycji w prace badawczo-rozwojowe przez wprowadzenie specjalnych pakietów korzyści dla firm angażujących się w partnerstwo w ramach regionalnych lub centralnych ośrodków cyberbezpieczeństwa;
- Pobudzić zainteresowanie sektora publicznego krajowymi produktami w zakresie cyberbezpieczeństwa oraz zwiększyć otwartość administracji centralnej na współpracę z przedsiębiorstwami różnego rozmiaru: startupami, MŚP oraz krajowymi liderami;
- Zreformować ramy prawne tak, aby umożliwić wszystkim firmom krajowym, w tym startupom i MŚP, udział w przetargach publicznych na produkty i usługi w dziedzinie cyberbezpieczeństwa;
- Zaprojektować i zrealizować długoterminową strategię PR w celu promowania Polski jako centrum kompetencji w dziedzinie cyberbezpieczeństwa.

ŹRÓDŁA:

1. European Commission, DG Justice, *Freedom and Security, Final Report On Study on Critical Dependencies of Energy, Finance and Transport Infrastructures on ICT Infrastructure*, 2009, [online]www.ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/docs/pdf/2009_dependencies_en.pdf (access: 12/05/2017), p. 10.
2. Martin C. Libicki,*Conquest in Cyberspace: National Security and Information Warfare*, Cambridge University Press, New York 2007.
3. Fortune, Global 500, Technology sector, 2016, [online] www.beta.fortune.com/global500/list/filtered?sector=Technology (access: 12/05/2017).
4. International Telecommunication Union, *Global Cybersecurity Index &Cyberwellness Profiles*, 2015, [online] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (access: 12/05/2017).
5. Bloomberg Innovation Index, High Tech Companies, 2015, [online] www.bloomberg.com/graphics/2015-innovative-countries/ (access: 12/05/2017).
6. Symantec, *Internet Security Threat Report*, April 2017, Vol. 22, [online] www.symantec.com/content/dam/symantec/docs/reports/istr-22-2017-en.pdf (access: 12/05/2017).
7. Hackmageddon, 2016 Cyber Attacks Statistics, [online] www.hackmageddon.com/2017/01/19/2016-cyber-attacks-statistics/ (access: 12/05/2017).
8. Cybersecurity Ventures, The Cybersecurity 500, 2017, [online] www.cybersecurityventures.com/cybersecurity-500-list/ (access: 12/05/2017).
9. F-Secure, *The State of Cyber Security 2017*, Report, 2017, [online] www.business.f-secure.com/the-state-of-cyber-security-2017; PWC, *The Global State of Information Security*, Survey 2017, [online] www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html (access: 12/05/2017).
10. Gartner, Forecast Analysis: Information Security, Worldwide, 1Q16 Update, 2016, [online] www.gartner.com/doc/3357452;Visiongain, Cyber Security Market Report 2016-2021, 2016, [online] https://www.visiongain.com/Report/1583/Cyber-Security-Market-Report-2016-2021; Cybersecurity Ventures, Cybersecurity Market Report Q1 2017, 2017, [online] http://cybersecurityventures.com/cybersecurity-market-report/; 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, [online] www.marketsandmarkets.com/PressReleases/cyber-security.asp (access: 12/05/2017).
11. Abomhara M., Geir M. Køien. 2015. *Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks,"*Journal of Cyber Security and Mobility" 2015, 4 (1),pp. 65–88; CamhiJ.,Business Insider, *BI Intelligence projects 34 billion devices will be connected by 2020*, 2015, [online] www.businessinsider.com/bi-intelligence-34-billion-connected-devices-2020-2015-11?IR=T (access: 12/05/2017).
12. Intel Security, Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, June 2014, [online] https://www.mcafee.com/tw/resources/reports/rp-economic-impact-cybercrime2.pdf (access: 12/05/2017).
13. Cybersecurity Ventures, 2016 Cybercrime Report, [online] www.cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ (access: 12/05/2017).
14. SC Magazine UK, *S&P could downgrade lenders to standard and poor for cyber-security*, 2015, [online] www.scmagazineuk.com/standard-and-poor-to-downgrade-banks-credit-rating/article/534298/ (access: 12/05/2017).
15. OnMSFT, *China is reportedly not banning Microsoft Office after all*, 2014, [online] www.onmsft.com/news/china-not-banning-microsoft-office-suite (access: 12/05/2017).
16. Brown G., *Spying and Fighting in Cyberspace: What Is Which? "*Journal of National Security Law & Policy"2016, 8 (3): 621–43; BBC, *Huawei boss says US ban 'not very import*ant, 2014, [online] www.bbc.com/news/business-29620442 (access: 12/05/2017).

17. CSO, *Cybersecurity job market to suffer severe workforce shortage*, 2015, [online] www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html (access: 12/05/2017).
18. European Cyber Security Organisation, European Cybersecurity PPP, Presentation of Luigi Rebuffi Secretary General at ECSO, 2016, [online] www.enisa.europa.eu/events/enisa-validation-workshop-market-study-of-nis-products-and-services/3TheDSMandcPPPinitiativeLuigiRebuffi.pdf (access: 12/05/2017).
19. PMR, *Rynek IT w Polsce 2016. Analiza rynku i prognozy rozwoju na lata 2016-2021*, 2016, [online] www.pmrpublications.com/product/Rynek-IT-w-Polsce-2016(access: 12/05/2017).
20. Ministerstwo Rozwoju, *Polski Sektor ICT*, 2017, [online] https://www.mr.gov.pl/strony/aktualnosci/perspektywy-rozwoju-polskiej-branzy-ict-do-roku-2025-raport-ministerstwa-rozwoju/.
21. Hacker Rank, *Which Country Would Win in the Programming Olympics?*, 2017, [online]www.blog.hackerrank.com/which-country-would-win-in-the-programming-olympics/ (access: 12/05/2017).
22. Hacker Rank, *Where Should You Open Your Next Engineering Office?*, 2017, [online] www.blog.hackerrank.com/open-next-engineering-office/ (access: 12/05/2017).
23. Dziennik Internautów Technologie, *Polska kształci za mało informatyków. Umiejętność programowania najbardziej poszukiwaną kompetencją na rynku pracy, 2015*, [online] www.di.com.pl/polska-ksztalci-za-malo-informatykow-umiejetnosc-programowania-najbardziej-poszukiwana-kompetencja-na-rynku-pracy-53442 (access: 12/05/2017).
24. Lewandowska M.S., *Barriers to Innovation in Poland Compared with Other European Countries: Implications for Innovation Policy* [in:] *Poland Competitiveness Report 2016. The Role Of Economic Policy And Institutions*, ed. M.A. Weresa, World Economy Research Institute, SGH Warsaw School Of Economics, Warsaw 2016, [online] www.kolegia.sgh.waw.pl/pl/KGS/struktura/IGS-KGS/publikacje/Documents/Raport_POLAND2016.pdf (access: 12/05/2017), p. 214.
25. PMR, *Rynek IT w Polsce 2016…*, op.cit.
26. Instytut Badań Strukturalnych, *Finanse Publiczne w Polsce – diagnoza na tle innych krajów*, IBS policy paper 04/2016, 2016, [online] www.ibs.org.pl/app/uploads/2016/04/IBS_Policy_Paper_04_2016_pl.pdf (access: 12/05/2017).
27. Wprost, 200 Największych Polskich Firm 2015, 2015, [online] www.rankingi.wprost.pl/200-najwiekszych-firm (access: 12/05/2017).
28. WNP portal gospodarczy, *Tauron rozważa utworzenie funduszu typu CVC*, 2016, [online] www.energetyka.wnp.pl/tauron-rozwaza-utworzenie-funduszu-typu-cvc,275967_1_0_0.html (access: 12/05/2017).
29. Rzeczpospolita, *Witelo stawia na innowacje*, 2017, [online] www.rp.pl/Ubezpieczenia/303019897-Witelo-stawia-na-innowacje.html (access: 12/05/2017).
30. MinisterstwoRozwoju, *Responsible Development Plan*, presentation, 2016, [online] www.mr.gov.pl/media/14873/Responsible_Development_Plan.pdf (access: 12/05/2017).
31. Portal CYBERSEC HUB, [online] www.cybersechub.eu (access: 12/05/2017).

AUTORZY

CDR Wiesław Goździewicz (Polish Navy)

Radca Prawny w NATO Joint Force Training Centre w Bydgoszczy

W 2002 roku ukończył Wydział Prawa i Administracji Uniwersytetu Gdańskiego, następnie wstąpił do Sił Zbrojnych i rozpoczął zawodową służbę wojskową jako referent prawny w 43. Bazie Lotniczej Marynarki Wojennej. Służył również w Oddziale Prawa Międzynarodowego Publicznego Departamentu Prawnego Ministerstwa Obrony Narodowej. W październiku 2009 został przydzielony do Joint Force Training Centre w Bydgoszczy.

Poza codzienną obsługa prawną JFTC, prowadzi szkolenia na temat praktycznych aspektów międzynarodowego prawa humanitarnego i prawnych aspektów operacji wojskowych, zarówno w kontekście działań konwencjonalnych jak i operacji cybernetycznych i operacji w przestrzeni kosmicznej.

Cyprian Gutkowski

Prawnik

Ukończył Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie (Wydział Prawa i Administracji), oraz podyplomowe studia w Szkole Głównej Handlowej w Warszawie na kierunku Zarządzanie Bezpieczeństwem Informacji. Doświadczony prawnik, który jest w stanie doradzać w zakresie prawa, procedur jak i cyberbezpieczeństwa. Jest ekspertem w zakresie ochrony danych osobowych. Współpracuje z rządem polskim i organizacjami pozarządowymi w zakresie, cyberbezpieczeństwa, prawa i procedur bezpieczeństwa informacji.

Robert Siudak

Ekspert Instytutu Kościuszki

Koordynator projektu CYBERSEC HUB oraz redaktor naczelny kwartalnika European Cybersecurity Market. Cybersechub.eu stanowi platformę łączącą innowacyjne startupy z Europy Środokowo-Wschodniej, inwestorów, ośrodki akademickie oraz lokalne i centralne władze w celu stworzenia regionalnego centrum kompetencji w dziedzinie cyberbezpieczeństwa. Organizator Startup Stage podczas corocznego Europejskiego Forum

Cyberbezpieczeństwa CYBERSEC stanowiącego jedną z najważniejszych konferencji public policy w tematyce bezpieczeństwa ICT. Studiował w Izraelu oraz Irlandii, aktualnie kończy studia doktoranckie na Uniwersytecie Jagiellońskim. Autor dwóch monografii oraz szeregu artykułów opisujących wpływ nowych technologii na bezpieczeństwo narodowe oraz międzynarodowe.

Lior Tabansky

Pracownik naukowy w Blavatnik Interdisciplinary Cyber Research Center, Uniwersytet Telawiwski. Obecnie jest Dyrektorem ds. Strategii w Cyber Security Group – firmie doradczej z Tel Avivu.

Lior prezentuje unikalną strategiczną metodologię cyberbezpieczeństwa, popartą ekspertyzą w dziedzinie nauk politycznych i studiów nad bezpieczeństwem (obrona rozprawy doktorskiej przewidziana na rok 2017), doświadczeniem zdobytym w think-tankach, instytucjach publicznych i prywatnych wysokiego szczebla oraz piętnastoletnią profesjonalną praktyką w sektorze IT.

Jest współautorem wydanej niedawno książki Cybersecurity in Israel napisanej wspólnie z Profesorem Ben-Israelem. Cybersecurity in Israel jest pierwszym kompleksowym sprawozdaniem dotyczącym ewolucji polityki cyberbezpieczeństwa Izraela, związanych z nią dylematów i działań na przestrzeni dziesięcioleci z perspektywy wtajemniczonego w te procesy eksperta.

Lior Tabansky rozwija także unikatową analizę roli, jaką całościowa strategia i krajowy system innowacyjny odgrywają w cyberbezpieczeństwie.

PARTNER PUBLIKACJI

Asseco Poland jest największą firmą informatyczną notowaną na Giełdzie Papierów Wartościowych w Warszawie. Od ponad 25 lat tworzy zaawansowane technologicznie oprogramowanie dla firm i instytucji z kluczowych sektorów gospodarki. To obecnie największa spółka informatyczna w Europie Środkowej oraz szósty producent oprogramowania w Europie. Grupa Asseco działa w 54 krajach. Zatrudnia ponad 22 tys. osób. Tworzy technologie, które wspierają funkcjonowanie, a także rozwój ponad 100 000 firm i organizacji. Działając na międzynarodowych rynkach, Asseco zbiera wszechstronne doświadczenia, które tworzą know-how wszystkich firm z Grupy. Synergia tych kompetencji stanowi wartość dodaną dla klientów firmy, którzy otrzymują produkty najwyższej jakości.

O WYDAWCY

Instytut Kościuszki to wiodący pozarządowy ośrodek naukowo-badawczy o charakterze non-profit założony w 2000 r. Naszą misją jest działanie na rzecz społeczno-gospodarczego rozwoju i bezpieczeństwa Polski, jako aktywnego członka Unii Europejskiej oraz NATO.

Instytut Kościuszki specjalizuje się w tworzeniu strategicznych rekomendacji i kierunków rozwoju kluczowych polityk publicznych, stanowiących merytoryczne wsparcie dla polskich i europejskich decydentów politycznych. Raporty i analizy przygotowywane przez ekspertów think tanku są niezależne i apolityczne, a ich konkluzje są istotnym źródłem informacji dla sektora prywatnego i społeczeństwa obywatelskiego.

Jako lider wśród polskich organizacji pozarządowych, Instytut Kościuszki realizuje szereg krajowych i międzynarodowych projektów poświęconych wieloaspektowo rozumianej tematyce bezpieczeństwa, w tym bezpieczeństwa energetycznego, gospodarczego oraz cyberbezpieczeństwa. Angażując do współpracy kluczowych interesariuszy polityki i biznesu, a także przedstawicieli organizacji międzynarodowych oraz sektora NGO, Instytut inicjuje społeczno-polityczną debatę nad najważniejszymi wyzwaniami dla Polski i Europy.

Dzięki swej wiodącej pozycji, Instytut Kościuszki przyciąga najlepszych analityków z całego świata, dając tym samym początek wielu pionierskim i innowacyjnym przedsięwzięciom. Instytut Kościuszki jest pomysłodawcą i głównym organizatorem Europejskiego Forum Cyberbezpieczeństwa – CYBERSEC, corocznej konferencji poświęconej strategicznym aspektom cyberprzestrzeni, której pierwsza edycja odbyła się w 2015 r. Wydarzenie stanowi platformę regularnego dialogu pomiędzy kluczowymi interesariuszami i uznane zostało w rankingu Concise Courses za jedną z pięciu najważniejszych konferencji tego typu w Europie. W ramach projektu CYBERSEC, powstała również krajowa odsłona przedsięwzięcia – Polskie Forum Cyberbezpieczeństwa – CYBERSEC PL.

Partner

asseco

ISBN: 978-83-63712-30-3

INSTYTUT KOŚCIUSZKI