aut. Andrzej Kozłowski 30.07.2018

CYBERBEZPIECZEŃSTWO SIŁĄ NAPĘDOWĄ POLSKIEJ INNOWACJI? [ANALIZA]

W Polsce temat innowacji i nowoczesnych technologii staje się coraz popularniejszy. Często mówi się, że mamy świetne kadry, potencjał i naturalną zdolność do wymyślania koła na nowo". Przykładów rewolucyjnych wynalazków będących dziełem Polaków nie brakuje. Jan Szczepaniak i Kazimierz Żeglań wynaleźli kamizelkę kuloodporną, Mieczysław Wolfe był jednym z twórców hologramu. Polacy opracowali również metody pozyskiwania dużych ilości grafenu. Niestety rozwiązania te nie zostały skomercjalizowane. Wydawać by się mogło, że kwestie cyfrowe to najlepszy obszar do rozwoju, a Polacy to prawdziwi „kilerzy IT" i że nic nie stoi na przeszkodzie, żeby wyznaczać kierunki. Czy jednak faktycznie tak jest?

Niebieski laser – historia na przyszłość. Problem z innowacjami w Polsce

Warto jest wspomnieć o wynalazku niebieskiego laseru, ponieważ ten przykład dość dobrze ilustruje problem polskich badań i rozwoju (B+R). Na początku XXI wieku polskim naukowcom udało się stworzyć niebieski laser na podłożu azotku galu, który miał dać dużą przewagę nad konkurencją. W 2002 roku Prezydent Aleksander Kwaśniewski przyznał naukowcom pracującym nad tym projektem nagrodę w kategorii „Najlepszy wynalazek w dziedzinie produktu lub technologii", a media zastanawiały się gdzie można zastosować rewolucyjną technologię. W tym samym czasie w Japonii opracowano identyczną technologię i rozpoczęto jej sprzedaż. Okazało się, że pomimo wsparcia finansowego ze strony państwa, program rozwoju lasera był realizowany po omacku, bez żadnego harmonogramu prac i koordynacji. Konkurencja zaczęła komercjalizować swoje pomysły, a Polacy zostali z kilkoma prototypami, które nadawały się jedynie do zastosowania laboratoryjnego. Przykład ten ilustruje wiele problemów, które napotyka innowacyjność w Polsce.

Niestety na tle innych państw naszemu państwu daleko do pozycji lidera jeśli chodzi o nakłady na badania i rozwój (B+R). Unia Europejska wydaje na nie 2 proc. PKB, a Polska tylko 0.97. W ostatnim Globalnym Indeksie Innowacji Polska uplasowała się na 38 pozycji z pośród 127 badanych państw. Przykładowo Czechy zajęły 24 miejsce. Według ekspertów sytuacja ta ulegnie zmianie, ponieważ na wzrost zainteresowania polskich przedsiębiorców działalnością B+R powinny wpłynąć zachęty podatkowe oraz wsparcie bezzwrotnymi dotacjami. Innymi czynnikami jest też rosnąca świadomość konieczności dostosowania oferty do dynamicznie zmieniającego się otoczenia, ze względu na postęp technologiczny. W 2017 roku ¼ polskich firm, które wzięły udział w badaniu Deloitte poinformowała, że nie wydaje na B+R żadnych pieniędzy.

Zwiększenie wydatków na B+R wiąże się nie tylko ze zmianą świadomości, ale przede wszystkim zmianą w odpowiedniej legislacji. Największym problemem hamującym korzystanie z zachęt w prowadzaniu działalności B+R są nieprzejrzyste przepisy – wynika z raportu Deloitte „Central European Corporate R&D Report 2018. Największym problemem jest tu zmienna interpretacja przepisów regulujących zasady korzystania z dostępnych instrumentów wsparcia. Firmy skarżą się również na niejasną ocenę organów podatkowych.

Brakuje odpowiedniego wykorzystania możliwości drzemiących w krajowych przedsiębiorstwach i ośrodkach akademickich. Według respondentów biorących udział w badaniu to właśnie dostępność doświadczonych kadr naukowych jest jednym z bodźców pozytywnie wpływających na B+R.

Z raportu Instytutu Kościuszki „Bezpieczeństwo poprzez innowacje" wynika, że problemem jest też niewystarczające finansowanie, zarówno wewnętrzne jak i zewnętrzne, łącznie z kapitałem wysokiego ryzyka. Jest on szczególnie potrzebny startupom, które chcą wprowadzić ofertę na rynek międzynarodowy. Zmusza to polskie startupy do szukania inwestycji na rynkach zagranicznych.

Raport firmy PMR o rynku IT w Polsce stwierdza, że problem leży w małym zapotrzebowaniu na B+R ze strony sektora publicznego, w tym władz centralnych i lokalnych, jak również przedsiębiorstw.

Rynek IT z pewnością jest dobrym obszarem w myśleniu o rozwoju i wprowadzaniu innowacyjnych technologii z dużą szansą na ich skomercjalizowanie. Duże możliwości z pewnością daje dynamicznie rozwijające się cyberbezpieczeństwo.

Cyberbezpieczeństwo – szansą na rozwój?

Cyberbezpieczeństwo bardzo często postrzegane jest w kategorii następnego, niepotrzebnego wydatku. Powinno być jednak rozważane jako potencjalny zysk. Globalny rynek cyberbezpieczeństwa w 2016 roku wynosił 120 mld. dolarów. W 2021 wartość ta osiągnie 240 mld dolarów. Wiele państw dostrzegło tą tendencje i traktuje cyberbezpieczeństwo jako kolejną inwestycję. Izraelski sektor cyberbezpieczeństwa generuje prawie 4 miliardy dolarów rocznie. W Wielkiej Brytanii suma ta wynosi 2 miliardy dolarów. Przykłady tych państw pokazują, że cyberbezpieczeństwo może być bardzo dochodowym biznesem.

Wartość polskiego sektora ICT w 2016 roku wyniosła 8.5 miliarda dolarów. W przeciągu ostatnich dwóch dekad obserwowaliśmy stały roczny wzrost na poziomie 5 – 6 %. Jest to spowodowane zmianą charakteru polskiej gospodarki, z opartej na przemyśle na taką, która nacisk kładzie na usługi, w tym rosnące usługi teleinformatyczne. Jak pisze Robert Siudak we wspomnianym już raporcie Instytutu Kościuszki, sektor ICT jest jednym z najbardziej konkurencyjnych na świecie sektorów polskiej gospodarki od startupów, przez średnie firmy, aż po wielkie przedsiębiorstwa. Polska jest też siedzibą dziesiątek rozwijających się na świecie marek. Wielu z nich to liderzy w swoich segmentach rynkowych, a ich działy badawczo-rozwojowe są źródłem innowacyjnych rozwiązań technologicznych.

Polska zajmuje 3 miejsce w światowym rankingu deweloperów. Polskie uniwersytety kształcą 30,000 specjalistów ICT rocznie. Liczby te robią wrażenie. Dodając do tego, że polscy informatycy i osoby odpowiedzialne za cyberbezpieczeństwo znajdują się w światowej czołówce, co potwierdzają poprzez wysokie miejsca w międzynarodowych zawodach – wynika z raportu Instytutu Kościuszki. Przykładowo HackerRank z 2017 roku plasuje Polskę na trzecim miejscu, tuż za Chinami i Rosją. Jak widać Polska ma idealną pozycję do rozwinięcie sektora cyberbezpieczeństwa i uczynienie z niego koła napędowego innowacji. Dodatkowo jako państwo UE może ona skorzystać z planu inwestycji w wysokości 1.8 mld euro w sektor cyberbezpieczeństwa do 2020 roku oraz jako członek NATO może wykorzystać takie mechanizmy jak NATO Industry Cyber Partnership wynika ze wspomnianego już raportu Instytutu Kościuszki. Polska musi tworzyć innowacyjne rozwiązania, bo inaczej pozostanie biernym odbiorcą technologii z zagranicy.

Rola państwa

Innowacje w technologiach IT i cyberbezpieczeństwa nie mogą rozwinąć się bez aktywnego zaangażowania państwa 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.

Państwo w ramach Krajowych Ram Polityki Bezpieczeństwa w cyberprzestrzeni na lata 2017-2022 w ramach trzeciego celu szczegółowego wyznaczyło zwiększenie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni. Wyodrębnienie budowy silnego sektora cyberbezpieczeństwa w ramach czterech głównych celów szczegółowych strategii świadczy o znaczeniu tego zagadnienia. Miejmy nadzieję, że za zapisami w strategii pójdą konkretne działania, ponieważ jak dotychczas partnerstwo publiczno-prywatne nie działało najlepiej w obszarze cyberbezpieczeństwa.

Nie tylko główny dokument strategiczny dotyczący problemu cyberbezpieczeństwa zwraca uwagę na ten problem. Kwestia R&D w cyberbezpieczeństwie stała się istotnym zagadnieniem w Strategii na rzecz Odpowiedzialnego Rozwoju, gdzie zaprezentowano „Cyberpark Enigma". Jego celem ma być rozwój kompetencji polskich firm i jednostek naukowo badawczych w dziedzinie cyberbezpieczeństwa i analizy danych. Projekt ma pozwolić na stworzenie ośrodka o potencjale pozwalającym konkurować z innymi firmami na europejskim rynku specjalistycznych usług IT. Przewidywana jest także poprawa infrastruktury informatycznej poprzez inwestycję w superkomputery oraz ośrodki typu data center. Ważnym celem jest również wykształcenie wysoce wykwalifikowanej kadry.

O znaczeniu cyberbezpieczeństwa mówił również premier Mateusz Morawiecki

Talenty informatyczne są naszym dobrem narodowym, chcemy to dobro narodowe włączyć w globalny krwioobieg gospodarczy, by cyberbezpieczeństwo stało się naszą narodową kompetencją, naszą specjalnością. *Deklaruję, że chcemy, by cyberbezpieczeństwo stało się naszą narodową kompetencją. Trzy polskie uniwersytety są w najściślejszej czołówce w programowaniu komputerowym, co pokazały akademickie mistrzostwa świata w tej dziedzinie.*

Dokumenty strategiczne czynią z rozwoju polskiego B+R jeden z priorytetów. Niestety nie widać jednak żadnych prób ich realizacji w praktyce. Źle wygląda też współpraca publiczno-prywatna o czym wspomina raport Instytutu Kościuszki. 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 – piszą autorzy raportu. Problem leży też w innym podejściu do współpracy publiczno-prywatnej. Opiera się ono w dużej mierze na samorządach, które zawarły aż 103 ze 112 umów (92 %), Do końca 2016 roku zawarto zaledwie 5 kontraktów, których stroną była administracja rządowa. Cyberbezpieczeństwo nie może być realizowane na poziomie lokalnym.

Ważną rolę pełnią też programy takie jak Bridge Alfa czy Starter, które łączą kapitał prywatny z publicznym. Są częścią szerszego programu wsparcia dla startupów pod hasłem Start in Poland. Należy również wspomnieć o funduszu Witelo, który jest wykorzystywany do inwestowania publicznych środków w polskie startupy.

Administracja rządowa powinna również podjąć odpowiednie działania do zwiększenia dostępności doświadczonych kadr naukowych, poprzez proponowanie naukowcom konkurencyjnych warunków pracy. W ten sposób będzie można również sprowadzić do kraju osoby, które wyemigrowały. Bez wsparcia dla szkolnictwa wyższego nie udało się rozwinąć innowacyjności w kraju.

Rząd powinien również dokonać zmian w prawie, dostosowując środowisko regulacyjne w celu uczynienia go bardziej przyjaznym dla innowacyjnych firm. Wprowadzenie ulg podatkowych jest z pewnością dobrym pomysłem, ale również ważne jak nie ważniejsze jest stworzenie przejrzystych

zasad korzystania z nich.

Wybrane technologie rozwinięte przez polskie firmy

Jednym z rozwiązań, które rozwinęły polskie firmy są technologie antyDDoS. Pierwszym z nich był system redGuardian firmy Atende Software. Jest to usługa oferowana w chmurze. Dzięki globalnej sieci centrów filtrowania, działających w oparciu o autorskie oprogramowanie, atak jest zatrzymywany możliwie blisko jego źródła. W momencie aktywacji usługi, adresacja IP klienta jest rozgłaszana przy pomocy protokołu BGP jednocześnie we wszystkich centrach filtrowania, co skutkuje skierowaniem do nich całego ruchu klienta.

Dynamicznie w obszarze B+R działa Exatel. Nowa strategia rozwojowa, która została wprowadzona kładzie szczególny nacisk na kompetencje badawczo-rozwojowe. Udało mu się pozyskać z grantów prawie 11 milionów złotych.

Pozwoliło to Exatelowi na rozwinięcie własnego systemu obrony przez zagrożeniami DDoS, pisanego od początku z myślą o potrzebach dużego operatora telekomunikacyjnego o skali europejskiej. Projekt TAMA będzie wykorzystywał algorytmy i technologie opracowywane przez EXATEL przy współpracy z Politechniką Warszawską. Wkładem operatora będzie także zaawansowana infrastruktura sieciowa oraz doświadczony zespół specjalistów od projektów IT, cyberbezpieczeństwa (SOC) i telekomunikacji. Tylko połączone kompetencje naukowców, informatyków i łącznościowców mogą dać w efekcie działający system zdolny do radzenia sobie z gigabitowym atakiem (o przepustowości ponad 100 Gb/s). W codziennej praktyce Exatel ruch sieciowy jest bowiem badany na wielu poziomach – od składni pojedynczego pakietu, przez zachowanie lokalnych sieci do technik informatyki śledczej i inżynierii wstecznej szkodliwego oprogramowania. Całkowita kontrola operatora nad kodem źródłowym rozwiązania zapewni wyższy poziom bezpieczeństwa w stosunku do rozwiązań importowanych, co jest niezwykle ważne z punktu widzenia np. ochrony infrastruktury krytycznej.

Exatel rozwija dynamicznie sieć 5G, która obecnie testowana jest w przestrzeni publicznej w ramach dużego konsorcjum naukowo-biznesowego RAPID 5G Wcześniej żadna polska firma się tym nie zajmowała. Sieć 5G wejdzie w 100% w życie i będzie to ogromny przełom dla rozwoju technologii. Exatel w ten sposób ma zamiar ustalać przyszłe standardy i zasady gry a potem oczywiście czerpać z tego korzyści. W przyszłości Exatel ma zamiar pracować nad opracowaniem środowiska 5G dla takich usług jak AR/VR czy holografia.

Operator pracuje też nad rozwiązaniem nazwanym programowalna sieć komputerowa (Software Defined Network – SDN) wraz z inną polską firmą ENAMOR International. Są to nowe rozwiązania, które będą w przyszłości kręgosłupem w telekomunikacji i cyberbezpieczeństwie i z dużą dozą pewności nastąpi zmiana a SDN zastąpi standardowe rozwiązania hardware. Exatel na rozwój tego pomysłu otrzymał grant z Narodowego Centrum Badań i Rozwoju. Polsko-polskie konsorcjum spowoduje, że efekty zostaną w kraju, co powinno być celem tych starań. Prace nad rozwiązaniem SDN są niestety odzwierciedleniem polskiego R+B, który cechuje innowacyjny marazm czy strach przed podejmowaniem ryzyka. Wcześniej nikt nie podejmował pracy nad tą technologią, bo oznaczało by to pójście w nieznane. Telekomunikacja jest przykładem obszaru otwartego na zmiany. Takiego, w którym polskie firmy z roli konsumentów technologii mogą i powinny wchodzić w rolę partnerów technologicznych.

Exatel współpracuje z Politechniką Warszawską, gigantami typu CISCO czy Verizon i służbami. W ten sposób realizuje w praktyce dobry model współpracy z administracją publiczną, sektorem naukowym i innymi przedsiębiorstwami z obszaru IT.

Warto również wspomnieć o polskim szyfrującym komunikatorze UseCrypt Messenger, który jest

jedynym polskim produktem tego typu. Korzysta on z autorskich zabezpieczeń, gwarantujących pełną prywatność przesłanych informacji, aby wykluczyć ryzyka posłuchu czy ataku hakerskiego.

Powyższe przykłady pokazują, że polskie firmy IT próbują wprowadzić autorskie, rozwiązania komercyjne oparte na nowej technologii na rynek i radzą sobie z tym całkiem nieźle. Polska ma jednak potencjał do tego, żeby takich wynalazków było jeszcze więcej.

Zakończenie

Pomimo zapowiedzi, że polski rynek IT staje się centrum świata, nie znajduje to potwierdzenia w konkretnych działaniach. Wciąż raczej jesteśmy na początku drogi. Należy też mierzyć siły na zamiary i nie próbować tworzyć własnych rozwiązań skomplikowanych technologii jak np. procesory. Nie oznacza to jednak, że polskie firmy nie mają możliwości stworzenia czegoś nowoczesnego i praktycznego, czyli technologii, która umożliwi polskim firmom możliwość zarobku. Atende, UseCrypt czy przede wszystkim Exatel to udowadniają.