# OFENSYWNY IZRAEL W CYBERPRZESTRZENI. EKSPERT: KLUCZEM START-UPY I WSPARCIE PAŃSTWA [WYWIAD]

**O fenomenie izraelskiego systemu cyberbezpieczeństwa, innowacyjnych start-upach i największych wyzwaniach w świecie wirtualnym mówi w wywiadzie dla Cyberdefence24.pl Lior Tabansky.**

**Andrzej Kozłowski: Izrael jest postrzegany jako państwo z jednym z najbardziej efektywnych i skutecznych systemów cyberbezpieczeństwa. Dlaczego?**

**Lior Tabansky:** Należy tu podkreślić wielką strategię bezpieczeństwa narodowego. Geopolityczna sytuacja Izraela jest niezwykle trudna. Od początku istnienia naszego państwa celem polityków i wojskowych było znalezienie sposobu na zrównoważenie przewagi ilościowej potencjalnych przeciwników poprzez stawianie na jakość wyposażenia i wyszkolenia. Była to jedyna możliwość przetrwania Izraela.

Dlatego też państwo inwestowało znaczne sumy pieniędzy w naukę i rozwój nowych technologii, ze szczególnym naciskiem na innowacyjne podejście, nie tylko skupiające się na czysto technicznej stronie. W 1967 roku Francja – główny dostawca uzbrojenia – nałożyła embargo na transport zaawansowanej broni do Izraela. Zmusiło to jego rząd do zwiększenia inwestycji w rozwój własnego przemysłu zbrojeniowego, który początkowo nie przynosił zysków, wręcz odwrotnie – sprawiał poważne problemy gospodarcze. Ostatecznie jednak doprowadził do powstania ludzkiego kapitału oraz infrastruktury umożliwiającej rozwój elektroniki. Była ona postrzegana jako element zwiększający siłę wojska izraelskiego. Doprowadziło to do powstania zaawansowanych ekspertyz i innowacji dotyczących komputerów, elektroniki i oprogramowania.

**Czytaj też:** Izrael będzie chętniej sprzedawał swoją cyberbroń

Kiedy w Izraelu mierzyliśmy się z problemem "co zrobić?", to postanowiliśmy oprzeć nasze cyberbezpieczeństwo na wcześniej rozwiniętych technologiach informacyjnych. Dzięki temu mieliśmy fundamenty oraz zdolności do działania w środowisku wirtualnym.

**A. K.: Wspomniał Pan o trudnym położeniu geopolitycznym Izraela. Jakie rodzaje zagrożeń postrzega się za najgroźniejsze dla kraju w świecie wirtualnym?**

L. T.: To połączenie działań państw i organizacji cyberprzestępczych. Państwa mają motywację i odpowiednie służby gotowe do przeprowadzenia takich działań. Cyberprzestępcy również mogą posiadać zaawansowane umiejętności. Inne organizacje i pojedynczy użytkownicy nie są postrzegani jako główne zagrożenie.

**A. K.: Wiele się mówi o sukcesie start-upów w obszarze cyberbezpieczeństwa w Izraelu, które następnie kupowane są przez duże zagraniczne podmioty. Co jest źródłem takiego olbrzymiego sukcesu?**

L. T.: Są dwie istotne rzeczy związane z cyberbezpieczeństwem i sukcesem naszych start-upów. Pierwszym z nich jest system edukacyjny, który zachęca osoby do samodzielności i kreatywności, a drugim są potrzeby naszego bezpieczeństwa. Musimy być tak mądrzy i skuteczni, jak to jest tylko możliwe.

Rozwój start-upów jest rezultatem świadomej polityki rządowej sięgającej lat 80. i początku 90. Polegała ona na wykorzystaniu innowacyjnego kapitału ludzkiego w celu rozwoju gospodarczego. Wszystkie instrumenty rządowe, jak np. prawo, wspierają innowacyjne rozwiązania. Prywatny kapitał dostarcza większość funduszy. Wielonarodowe korporacje prowadzą dojrzałą politykę w skali światowej, a start-upy kierują centrami w Izraelu. Dlatego że zdecydowanie lepiej rozumieją one specyficzny, izraelski ekosystem, który wytwarza wiele innowacyjnych rozwiązań. Nawet po zakupie start-upów przez wielkie firmy najzdolniejsi pracownicy zostają w Izraelu, nie są zabierani do Doliny Krzemowej. Jest to dla nas dobre, ponieważ ci ludzie mogą pomóc bronić Izrael przed zagrożeniami w cyberprzestrzeni.

**A. K.: Jakie zdolności ofensywne posiada Izrael i kto jest odpowiedzialny za ich przeprowadzanie?**

L. T.: Izraelskie Siły Obronne oraz wywiad odpowiedzialne są za przeprowadzanie takich operacji. Przeprowadziły one jedną z pierwszych ofensyw w cyberprzestrzeni, wciąż inwestują i rozwijają swoje zdolności w tym obszarze, ponieważ może to zapewnić przewagę jakościową nad przeciwnikiem. Większość operacji jest jednak tajna.

**A. K.: Jakie operacje ofensywne przeprowadził w cyberprzestrzeni Izrael?**

L. T.: Obecnie w Izraelu dysktujemy głównie o dwóch operacjach. Pierwszą z nich jest nalot przeprowadzony na syryjski reaktor nuklearny w 2007 roku. Według niepotwierdzonych informacji dzięki wykorzystaniu złośliwego oprogramowania udało się zneutralizować system obrony powietrznej. Druga operacja została przeprowadzona przy współpracy z wywiadem amerykańskim, a celem był irańskich program wzbogacania uranu.

**A. K.: Jakie jest największe wyzwanie dla Izraela w cyberprzestrzeni?**

L. T.: Największym wyzwaniem jest obrona całego społeczeństwa, a nie tylko krytycznych systemów rządowych. Problemem politycznym i etycznym jest zbalansowanie bezpieczeństwa i wolności społeczeństwa.

**Lior Tabansky – badacz Blavatnik Interdisciplinary Cyber Research Center Uniwersytetu w Tel Awiwie**