KONGRES OBYWATELSKI

Jak odbudować suwerenność cyfrową Polski?

GEN. KRZYSZTOF BONDARYK
Pełnomocnik ds. Organizacji Systemu Bezpiecznej Łączności Państwowej,
Ministerstwo Spraw Wewnętrznych i Administracji

W cyfrowym świecie państwo bez własnej kryptologii jest jak armia bez szyfrów – bezbronne, uzależnione, pozbawione suwerenności. Polska, choć ma tradycje sięgające Enigmy, oddała kontrolę nad informacją w obce ręce. Kluczowe technologie są dziś tworzone za granicą, obsługiwane przez zagranicznych dostawców i nie zawsze dostępne dla nas na własnych warunkach. Kto dobrze nie szyfruje po swojemu, ten zostanie odszyfrowywany przez innych.

W dobie postępującej cyfryzacji oraz rosnącego uzależnienia społeczeństw i państw od globalnej sieci, zdolność do skutecznej ochrony informacji stała się kluczowym czynnikiem wpływającym na poziom bezpieczeństwa oraz znaczenie i konkurencyjność państwa na arenie międzynarodowej. Szczególnej rangi nabrała ochrona informacji wrażliwych – gromadzonych masowo zbiorów danych: osobowych, finansowych, transakcyjnych etc.. Nie chodzi bowiem wyłącznie o dane wartościowe dla obcych państw z perspektywy wywiadowczej. Dane z różnego typu aktywności obywateli stały się dziś towarem, paliwem napędzającym rozwój sztucznej inteligencji (SI).

Nieautoryzowany i nieskrępowany dostęp do danych, w tym do tajemnic państwowych, może zagrozić interesom narodowym we wszystkich obszarach funkcjonowania państwa i przyczynić się do powstania zagrożeń politycznych, gospodarczych, a także niestabilności w obszarze społecznym. Szczególnie wrażliwym na nieautoryzowany dostęp zewnętrzny jest sektor militarny, od którego w dużym stopniu uzależnione są zdolności do obrony naszego kraju. Dlatego tak ważna jest zdolność do skutecznego utajnienia informacji wojskowych, planowania operacyjnego oraz zapewnienia bezpiecznej łączności na poziomie państwowym.

Kluczowe znaczenie dla utrzymania bezpieczeństwa militarnego ma zdolność do tworzenia i stosowania własnych, unikalnych rozwiązań – zwłaszcza narzędzi i algorytmów kryptograficznych. Stąd rosnące znaczenie kryptologii i potrzeba prowadzenia spójnej, skoordynowanej polityki państwa w tej dziedzinie.

Jej znaczenie dodatkowo wzrasta w kontekście szeroko zakrojonych operacji wywiadowczych prowadzonych przez liczne państwa

– również sojusznicze – w cyberprzestrzeni. Mowa tu o inwigilacji elektronicznych środków łączności oraz operacjach wpływu i dezinformacji w mediach społecznościowych. Skala tych działań, zależnie od potencjału kryptologicznego oraz przyjętej polityki państw, może mieć charakter globalny, regionalny lub wymierzony bezpośrednio w konkretne kraje. Celem tych działań pozostaje zawsze zdobycie informacji dających przewagę – negocjacyjną, militarną lub ekonomiczną. Pozyskiwanie danych często wymaga łamania zabezpieczeń, stosowania złośliwego oprogramowania czy wykorzystywania luk systemowych.

W erze cyfrowej ochrona danych to kwestia przetrwania państwa. Suwerenność informacyjna zaczyna się od własnej kryptologii, bo tylko narodowe algorytmy mogą zagwarantować, że strategiczne informacje nie trafią w niepowołane ręce.

Polska – jako państwo dysponujące znaczącym potencjałem gospodarczym, demograficznym i terytorialnym oraz będące ważnym członkiem NATO i UE, nie może pozostać bierna wobec tych zjawisk i procesów. Wojna w Ukrainie i realne zagrożenia dla naszej państwowości wymagają pilnych działań na rzecz zapewnienia suwerenności cyfrowej. Chodzi o zagwarantowanie pełnej kontroli nad systemami łączności i komunikacji oraz zapewnienia poufności przesyłanych informacji. Nie zapominajmy, że ta zasada powinna dotyczyć wszelkich nieuprawnionych podmiotów – również naszych sojuszników.

Drogą do tego celu jest odbudowa krajowych kompetencji i zdolności w dziedzinie kryptologii. Polskie systemy łączności państwowej – w tym systemy wojskowe – powinny być chronione przez polską kryptografię. Tylko wówczas możliwe będzie skuteczne zabezpieczenie ich przed zakłóceniem, przejęciem, podsłuchem czy dezaktywacją.

Polska kryptologia – wielkie zaniedbane dziedzictwo

Tradycje polskiej kryptologii sięgają XV wieku, kiedy to powszechną praktyką stało się w Polsce szyfrowanie korespondencji dyplomatycznej przez kancelarię królewską i hetmańską. W XVII i XVIII wieku służby królewskie regularnie przechwytywały i odszyfrowywały korespondencję przedstawicielstw dyplomatycznych innych państw działających na terenie Rzeczypospolitej. Sztuki szyfrowania uczono wówczas w kolegiach jezuickich.

Po odzyskaniu przez Polskę niepodległości po 1918 roku, duży nacisk położono na rozwój narodowej kryptologii. W czasie wojny polsko-bolszewickiej (1919–1921) istotną rolę odegrali kryptoanalitycy Sekcji Szyfrów Oddziału II Sztabu Generalnego Wojska Polskiego, którym udało się złamać ponad 100 szyfrów przeciwnika. Równocześnie polskie jednostki wojskowe korzystały wyłącznie z rodzimych systemów szyfrowania. W 1929 roku zorganizowano specjalny system kształcenia wybranych studentów matematyki z myślą o narodowej kryptologii. Natomiast w 1931 roku w Sztabie Generalnym WP powołano Biuro Szyfrów, odpowiedzialne za rozwój własnej kryptografii oraz analizę szyfrów radzieckich i niemieckich.

Poziom rozpoznania kryptografii radzieckiej był na tyle wysoki, że Polacy szkolili w tym zakresie nawet oficerów Imperialnego Sztabu Generalnego Japonii. Największe jednak osiągnięcia zanotował referat szyfrów niemieckich, w którym zatrudniono trzech młodych matematyków: Mariana Rejewskiego, Jerzego Różyckiego i Henryka Zygalskiego. Ich prace nad niemiecką maszyną szyfrującą Enigma doprowadziły do jej samodzielnego zrekonstruowania przez stronę polską. Od 1936 roku Biuro Szyfrów regularnie odczytywało depesze niemieckich sił lądowych, powietrznych i morskich, osiągając w 1938 roku skuteczność na poziomie około 65%. Umożliwiło to rozpoznanie 95% ugrupowania i planów operacyjnych sił niemieckich przed agresją we wrześniu 1939 roku. Osiągnięcia polskiej kryptologii zostały tuż przed wojną ujawnione przedstawicielom wywiadu francuskiego i brytyjskiego, co pozwoliło Brytyjczykom odpowiednio ukierunkować prace nad rozszyfrowywaniem Enigmy w ramach projektu „Ultra".

Po II wojnie światowej nastąpił upadek polskiej kryptografii – Polska korzystała głównie z rozwiązań radzieckich. Niemniej kryptoanaliza przez długi czas funkcjonowała jeszcze na wysokim poziomie, czego dowodem było m.in. złamanie przez kontrwywiad wojskowy jednego z amerykańskich szyfrów dyplomatycznych (w latach osiemdziesiątych).

Niestety, po transformacji ustrojowej w 1989 roku państwo nie potrafiło jasno wyartykułować swoich potrzeb w zakresie narodowej kryptologii. Skutkiem tego była praktyka zakupu gotowych rozwiązań kryptograficznych za granicą, w miejsce rozwijania własnych, rodzimych szyfrów i urządzeń. Nie zadbano przy tym o pozyskanie praw do ich modyfikacji czy serwisowania. Przyjęto zasadę, że rozwiązania „natowskie" są „z definicji" dobre. W wielu przypadkach kontrahenci zagraniczni nie oferowali zresztą wspomnianych możliwości, wykorzystując przewagę wynikającą z braku alternatyw w polskim sektorze.

Polska kryptologia, niegdyś światowy lider i twórca przełomowych rozwiązań, dziś zmaga się z uzależnieniem od zagranicznych technologii. Jest to efekt krótkowzrocznej polityki państwa – dyskontynuacji w procesie rozwijania własnych kompetencji i doświadczeń.

W efekcie tych decyzji Polska jest obecnie w znacznym stopniu uzależniona od zagranicznej kryptografii. Dotyczy to również Sił Zbrojnych RP, gdzie interoperacyjność systemów łączności z NATO zapewniana jest przez kryptograficzne urządzenia produkowane poza granicami kraju.

Znaczenie kodów źródłowych

W wyniku wieloletnich zaniedbań nastąpił znaczący regres w obszarze zdolności kryptoanalitycznych państwa. Brak zrozumienia tej problematyki wśród decydentów – zarówno polityków, jak i wojskowych – dobrze ilustruje podejście do kwestii tzw. „kodów źródłowych". Są one największym merytorycznym dobrem producenta – jego wizytówką – umożliwiającą weryfikację jakości produktu i rzetelności wykonawcy. Dostęp do kodów źródłowych pozwala zidentyfikować błędy, niedociągnięcia

i luki, które nie są wykrywalne w testach funkcjonalnych ani analizach podatności.

Gdyby strona polska miała dostęp do kodów źródłowych moglibyśmy sprawdzić czy w zakupionym sprzęcie nie znajdują się ukryte mechanizmy umożliwiające jego dezaktywację lub zdalne przejęcie kontroli. Niestety, w przypadku wielu zakupów uzbrojenia dokonywanych w ostatnich latach wykazano się daleko idącą niefrasobliwością. Zakładano dobrą wolę producenta, a jakość urządzeń, systemów i sterującego nimi oprogramowania weryfikowano jedynie na poziomie testów funkcjonalnych. Nie korzystano z przysługującego stronie zamawiającej prawa do pozyskania kodów źródłowych – nawet w sytuacji, gdy dostawcą był sojuszniczy kraj.

Co więcej, dokumentacja techniczna, która powinna być integralną częścią umów, pozostaje w Ministerstwie Obrony Narodowej rozproszona, nieskonsolidowana. Warto założyć, że potencjalni przeciwnicy militarni Polski mogą posiadać dostęp do kodów źródłowych części uzbrojenia i systemów wojskowych zakupionych przez naszą armię.

Pozyskanie kodów źródłowych musi stać się warunkiem wstępnym wszelkich negocjacji zakupowych za granicą. Powinien to być podstawowy test woli współpracy i otwartości kontrahenta. Depozytariuszem całej dokumentacji technicznej i kodów źródłowych dla urządzeń i systemów wojskowych powinna być wyodrębniona komórka Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni w Legionowie (dawniej: Narodowe Centrum Kryptologii).

Obowiązkowa weryfikacja kodów źródłowych i dokumentacji technicznej powinna obejmować: zgodność z zamówieniem (parametry, własność, typ, wersja, czasokres), bezpieczeństwo (jakość kodu, wyniki badań podatności) oraz podejście producenta do jakości i zgodności produktu z dokumentacją.

Kody źródłowe to nie przywilej, lecz warunek suwerenności – ich brak oznacza oddanie kontroli nad bezpieczeństwem sprzętu wojskowego w ręce zagranicznych producentów.

Działanie to wzmocni pozycję Polski wobec zagranicznych producentów uzbrojenia, zagwarantuje odpowiednią jakość i bezpieczeństwo sprzętu, a także umożliwi centralizację dokumentacji technicznej w jednym ośrodku kompetencyjnym. Jednocześnie pozwoli zaangażować krajowe ośrodki naukowo-badawcze w rozwój i audyt nowoczesnych rozwiązań technologicznych.

Luki w systemie prawnym

Podsumowując, należy stwierdzić, że brak świadomości władz państwowych co do znaczenia kryptologii dla bezpieczeństwa i suwerenności doprowadził do istotnego obniżenia kompetencji państwa w tym obszarze. A brak tej kompetencji uniemożliwia odzyskanie pełnej suwerenności – zwłaszcza władztwa nad zakupionym uzbrojeniem.

O braku polityki państwa w tym zakresie świadczą m.in. obowiązujące regulacje prawne. Ich charakterystyczną cechą jest niestosowanie terminu „kryptologia", mimo że odwołują się one do jej głównych dziedzin: kryptografii

i kryptoanalizy. Obowiązujące akty prawne nie określają w sposób kompleksowy polityki kryptologicznej państwa – nie wskazują jej celów, zasad, priorytetów ani instytucji odpowiedzialnych za jej wdrożenie. Traktują elementy kryptologii jako uzupełnienie rozwiązań technicznych, koncentrując się głównie na aspektach certyfikacji i akredytacji.

Brak polityki kryptologicznej państwa oznacza rezygnację z kontroli nad własnym bezpieczeństwem i suwerennością – to luka, którą pilnie trzeba wypełnić. Zmianie tej sytuacji nie sprzyjają luki w systemie prawnym (niekorzystne dla rodzimych firm) oraz praktyka instytucji publicznych w zakresie zamówień sprzętu i wyposażenia.

Dla porównania – pozytywnie oceniana dziś zdolność Turcji do produkcji nowoczesnego uzbrojenia wynika z jednoznacznie zdefiniowanej, państwowej polityki kryptologicznej, obowiązkowo wdrażanej zarówno w sferze cywilnej, jak i wojskowej.

W Polsce szczególną rolę odgrywa ustawa o ochronie informacji niejawnych. Niestety, nie sprzyja ona rozwojowi rodzimej kryptologii. W przypadku systemów służących do przetwarzania informacji niejawnych o klauzuli „zastrzeżone", dopuszcza możliwość uznania certyfikacji i akredytacji przeprowadzonych przez uprawnione instytucje państw NATO lub UE. Taka regulacja faworyzuje producentów zagranicznych.

Wojsko Polskie komunikuje się z NATO za pomocą zagranicznych systemów i urządzeń.

Dodatkowo, ustawa o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa mówi jedynie o monitorowaniu sprowadzanych do Polski rozwiązań kryptograficznych. Wprowadza to iluzję kontroli. Taka polityka szkodzi polskim producentom kryptografii, którzy nie są w stanie konkurować z masowym importem zagranicznych technologii.

Zakupy rozwiązań kryptograficznych odbywają się zazwyczaj w trybie ustawy o zamówieniach publicznych. Takie podejście sprawia, że energia instytucji państwowych koncentruje się na spełnieniu wymogów formalnych przetargu – pomijając kluczowe kwestie bezpieczeństwa i interesu narodowego. W praktyce prowadzi to do dyskryminacji polskich rozwiązań kryptograficznych oraz rodzimych produktów przemysłu informatycznego.

Reasumując: państwo polskie nie określiło swoich potrzeb i wymagań w zakresie narodowej kryptologii, w tym wojskowych norm kryptograficznych dla urządzeń i sprzętu będącego na wyposażeniu sił zbrojnych. Nie kontroluje procesów zachodzących w tej dziedzinie. Nie wprowadziło rozwiązań prawnych wspierających polską kryptografię, nie składa zamówień u rodzimych firm i nie promuje krajowych rozwiązań. Taka sytuacja wymaga pilnej zmiany.

Polski przemysł kryptograficzny

Obecnie Polska dysponuje ograniczonymi możliwościami wdrażania własnych rozwiązań kryptograficznych – zarówno w zakresie opracowywania algorytmów (z powodu niewystarczającej liczby wykształconych

kryptologów), jak i produkcji nowoczesnych urządzeń tego typu (mimo realnych potrzeb, brakuje zamówień sektora publicznego).

Wprawdzie polski przemysł i środowisko naukowe prowadzą prace nad budową narodowych rozwiązań kryptograficznych, jednak brak jednolitej koncepcji w zakresie projektowania i implementacji systemów chronionych kryptograficznie, a także tendencja wielu podmiotów państwowych i krajowych do korzystania z gotowych rozwiązań zagranicznych, sprawiają, że działania te przynoszą bardzo ograniczone efekty.

Brak koncepcji, mała skala zamówień, i niedobór wsparcia instytucjonalnego osłabił polski potencjał kryptograficzny, mimo że jeszcze dekadę temu istniały realne zdolności do tworzenia i wdrażania własnych rozwiązań.

Dodatkowym czynnikiem zniechęcającym krajowych producentów jest długotrwały i kosztowny proces certyfikacji urządzeń kryptograficznych w Polsce – prowadzony bez gwarancji późniejszych zamówień i wdrożeń. Brak narodowego ośrodka kompetencji w dziedzinie kryptologii oraz niska świadomość strategicznego znaczenia tej dziedziny doprowadziły do upowszechnienia praktyki pozyskiwania rozwiązań zagranicznych – zwłaszcza tych zapewniających interoperacyjność polskich Sił Zbrojnych z NATO.

Pomimo tych problemów, jeszcze dziesięć lat temu polski przemysł obronny posiadał realne zdolności w zakresie projektowania, produkcji i wdrażania krajowych urządzeń kryptograficznych – m.in. w postaci systemu identyfikacji „swój-obcy" oraz adaptacji polskich rozwiązań kryptograficznych w taktycznym systemie transmisji danych Link-16, w ramach realizowanych programów „Supraśl" i „Kwisa". Szkoda, że te kompetencje nie zostały należycie wykorzystane.

Duże ambicje, brak fundamentów

Na tle państw członkowskich NATO i UE, z których większość opiera się na własnych, samodzielnie opracowanych rozwiązaniach kryptograficznych, możliwości Polski prezentują się skromnie. Nasz kraj nie posiada własnej, sponsorowanej przez państwo polityki wspierania i stymulowania narodowej kryptologii – ani w wymiarze prawnym (własne standardy i normy kryptograficzne), ani naukowo-badawczym (rodzime ośrodki akademickie), ani badawczo-rozwojowym (centra technologiczne), ani produkcyjnym (przemysł), czy wdrożeniowym (implementacja krajowych rozwiązań kryptograficznych).

Taki stan rzeczy tworzy wyraźny dysonans między rzeczywistym poziomem polskiej kryptologii a ambicjami politycznymi RP w zakresie uzyskania istotnej pozycji w strukturach NATO i UE.

Działania naprawcze zostały podjęte przez Ministerstwo Obrony Narodowej dopiero w czerwcu 2013 roku, kiedy to powołano Narodowe Centrum Kryptologii (NCK) w celu konsolidacji zasobów kryptologicznych w Siłach Zbrojnych RP. Współpraca NCK z uczelniami wojskowymi i cywilnymi oraz realizacja projektu badawczo-rozwojowego

pod auspicjami Narodowego Centrum Badań i Rozwoju były ważnymi krokami i pozwoliły na stworzenie podstawowej infrastruktury w tej dziedzinie.

W NCK rozpoczęto także realizację projektu budowy Zintegrowanego Centrum Dystrybucyjno-Naprawczego (Service Depot) w Legionowie dla amerykańskiej kryptografii wykorzystywanej przez polską armię. Projekt ten, uzgodniony z partnerami amerykańskimi w 2014 roku, w przypadku powodzenia mógł znacząco zwiększyć zdolności obronne Polski – w stopniu przewyższającym symboliczne „dwie ciężkie brygady NATO" stacjonujące na terytorium RP.

Niestety, ze względu na brak wystarczającego wsparcia ze strony poprzedniego rządu, działania NCK przybrały ograniczoną skalę i okazały się niewystarczające do nadrobienia wieloletnich zaległości państwa. Co więcej, po 2015 roku zarzucono projekt serwisowania amerykańskiej kryptografii w Legionowie. Późniejsza konsolidacja zasobów NCK, wojsk łączności oraz Inspektoratu Informatyki MON w ramach Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni była odbierana raczej jako zabieg wizerunkowy, niż realna zmiana podejścia.

Nowe podejście do polityki kryptologicznej

Niezbędne jest uznanie kryptologii za jeden z filarów bezpieczeństwa państwa oraz ważny atrybut jego niepodległości i suwerenności. Konieczne jest przy tym zrozumienie, że rozwój kryptologii narodowej nie może być celem samym w sobie. Jego istotą powinno być wzmacnianie obronności państwa oraz ochrona jednego z fundamentów demokracji – prywatności obywateli, w szczególności ich danych osobowych oraz informacji przesyłanych drogą elektroniczną.

Polska kryptologia pozostaje w wyraźnym dysonansie wobec aspiracji państwa w NATO i UE – bez spójnej polityki, instytucji i wsparcia nie sposób zbudować kompetencji adekwatnych do ambicji.

W *Doktrynie Cyberbezpieczeństwa RP* z 2015 r., podpisanej przez Prezydenta Bronisława Komorowskiego, zapisano, że „strategicznym celem w obszarze cyberbezpieczeństwa RP, sformułowanym w Strategii Bezpieczeństwa Narodowego RP, jest zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni...". Kluczowym elementem realizacji tego celu powinno być uzyskanie przez państwo polskie pełnej jurysdykcji i suwerenności nad własną cyberprzestrzenią. Środkiem do jego osiągnięcia jest cyberbezpieczeństwo – nie jako cel sam w sobie, ale jako rezultat posiadania krajowych kompetencji i korzystania z zagranicznych technologii z dużą ostrożnością.

W tym kontekście kluczowe staje się ustanowienie narodowej polityki kryptologicznej, która określałaby cele, kierunki i zasady rozwoju kryptografii oraz kryptoanalizy, a także wspierałaby bezpieczeństwo w cyberprzestrzeni. Jej celem byłaby konsolidacja potencjału naukowego i przemysłowego oraz upowszechnienie zunifikowanych, narodowych rozwiązań

kryptograficznych w kluczowych sektorach państwa: obronności, telekomunikacji, energetyce, bankowości, łączności elektronicznej i transporcie. Również rozwój sztucznej inteligencji nie powinien się odbywać bez udziału polskiej kryptologii (kontrola nad algorytmami).

Polityka ta powinna regulować również zasady nadzoru państwa nad kryptologią narodową, uznając ją za integralną część systemu bezpieczeństwa i obronności. Należy wskazać instytucje odpowiedzialne za realizację polityki kryptologicznej oraz określić źródła i minimalne poziomy finansowania kryptologii w obszarach naukowo-badawczych, badawczo-wdrożeniowych oraz eksploatacyjnych. Szczególny nacisk powinien zostać położony na rozwój zasobów kadrowych – poprzez wspieranie kształcenia i utrzymywania ekspertów z dziedziny kryptologii.

Ostatecznie, polityka państwa powinna ukierunkowywać wysiłek przemysłu informatycznego na tworzenie perspektywicznych, ustandaryzowanych i zunifikowanych rozwiązań kryptograficznych. Państwo musi być zdolne do jednoznacznego zdefiniowania i wyartykułowania własnych potrzeb w zakresie narodowej kryptografii.

W tym celu konieczne jest wprowadzenie państwowych standardów i norm kryptograficznych. Trzeba również określić wymagania dotyczące implementacji polskich rozwiązań kryptograficznych zarówno w sektorze cywilnym, jak i wojskowym. Polityka państwa powinna również przejawiać się poprzez kierowanie zamówień publicznych do polskiego przemysłu kryptograficznego, przy jednoczesnym wprowadzeniu wymogu „twardej polonizacji" rozwiązań zagranicznych. Synergia tych działań pozwoli na odbudowę narodowych kompetencji kryptologicznych oraz na restaurację rynku krajowych rozwiązań kryptograficznych.

Rozwój kryptologii narodowej nie jest celem samym w sobie — to fundament suwerennego cyberbezpieczeństwa, warunek skutecznej obrony państwa i gwarancja ochrony prywatności obywateli.

Jurysdykcja cyfrowa i polska suwerenność

Polska – jako kraj, a także nasz przemysł oraz administracja cywilna i wojskowa – nie były zaangażowane w proces powstawania i konstruowania globalnej sieci.

- Polskie systemy telekomunikacyjne zostały jedynie podłączone do dynamicznie rozwijającej się sieci WWW.
- Modernizacja cyfrowa systemów teleinformatycznych w Polsce miała miejsce równolegle z prywatyzacją TP SA i rozwojem telefonii komórkowej. Adaptacja nowych usług, takich jak mobilny szerokopasmowy internet czy zminiaturyzowane urządzenia końcowe (smartfony, tablety), opierała się na sprzęcie i oprogramowaniu globalnych producentów. Analogiczne zjawisko dotyczy również urządzeń serwerowych, sieciowych i oprogramowania. Polski przemysł elektroniczny zasadniczo nie uczestniczył w globalnej produkcji poszczególnych składników infrastruktury internetowej.
- Administracja państwowa biernie towarzyszyła tym zmianom – nie pełniła

roli moderatora procesu modernizacji, który uwzględniałby interesy krajowego przemysłu i polskich rozwiązań technicznych. Występowała wyłącznie w roli użytkownika globalnej sieci.

- Obowiązujące w Polsce regulacje prawne pozostawiły kwestie architektury systemów TI – w tym wymagań wobec urządzeń i oprogramowania – wyłącznie w gestii dostawców, głównie globalnych korporacji. Wymóg interoperacyjności stał się wytrychem do narzucania producenckich standardów bigtechów. Kolejne polskie rządy rezygnowały z formułowania własnych wymagań sprzętowych, gwarantujących choćby minimalny poziom jurysdykcji – przynajmniej uprawnienia administratora lokalnego.
- Wieloletni brak rządowych (w tym militarnych) zamówień promujących rozwiązania krajowe, wspierających polską myśl naukowo-techniczną, spolszczających rozwiązania zagraniczne, a także brak państwowej polityki kryptologicznej – a co więcej: brak świadomości jak potrzebna jest taka polityka – świadczą o regresie w obszarze strategicznego myślenia wojskowego w Sztabie Generalnym. Wojsko nie zgłaszało zapotrzebowania na polskie rozwiązania w dziedzinie kryptografii, kryptoanalizy i dekryptażu. Zarząd Rozpoznania Wojskowego P-2 Sztabu Generalnego WP nie uwzględniał potrzeby dekryptażu obcych transmisji wojskowych w swoim zakresie działań.

Cyberbezpieczeństwo jest realizowane poprzez kompetencje: naukowo-badawcze, produkcyjne oraz zdolność do implementacji własnych rozwiązań. Kluczowe znaczenie mają w tym zakresie działania rządu oraz rozwój krajowego przemysłu elektronicznego i informatycznego. Państwo musi wykazać wolę działania i stworzyć odpowiednie ramy prawne dla rozwoju tych kompetencji. Rządowe zamówienia, szczególnie w sferze militarnej, powinny zawierać wymogi implementacji polskich rozwiązań i technologii – zarówno na poziomie aplikacji, algorytmów, jak i szeroko pojętego oprogramowania. W zakresie sprzętowym – urządzeń sieciowych i końcowych – preferencje powinny być przyznane krajowej produkcji, o ile jest to jeszcze możliwe. W obszarze protokołów telekomunikacyjnych i standardów – minimum to rozwijanie krajowych zdolności naukowo-badawczych i audytorskich.

W cyberprzestrzeni każde państwo staje się albo administratorem, albo użytkownikiem — Polska nie może pozostać tylko userem we własnej sieci – przyjęcie narodowej polityki kryptologicznej jest konieczne dla zachowania suwerenności cyfrowej.

Brak kompetencji i strategicznej perspektywy sprowadza debatę o cyberbezpieczeństwie na manowce. Polska coraz bardziej ulega przyspieszonej kolonizacji cyfrowej, preferując abonamentowe podejście do bezpieczeństwa. Wielkie korporacje oferują dziś „trójpak" – chmurę obliczeniową, sztuczną inteligencję oraz cyberbezpieczeństwo. Wystarczy wykupić abonament i zasilać obliczeniową chmurę własnymi danymi. W efekcie – w cyberprzestrzeni każdy jest albo *userem*, albo *adminem*. *Userem* może być nie tylko

pojedynczy obywatel, ale także całe państwo – każde, które zrzeknie się jurysdykcji nad własną cyberprzestrzenią.

Polska nie może zrezygnować ze swojej suwerenności cyfrowej. Jedyną drogą do jej utrzymania i odzyskania jest przyjęcie narodowej polityki kryptologicznej – opartej na krajowych rozwiązaniach, polskiej produkcji, własnych technologiach i pełnej jurysdykcji nad systemami teleinformatycznymi Rzeczypospolitej. ■

O AUTORZE

gen. bryg. w st. spocz. Krzysztof Bondaryk – uczestnik opozycji demokratycznej w PRL; w stanie wojennym więziony za naruszenie art. 46 i 48 Dekretu o Stanie Wojennym. W latach 1990–1996 szef białostockiej delegatury Urzędu Ochrony Państwa. W latach 1996–2001, pełniący funkcje kierownicze w MSWiA, m.in. jako Dyrektor departamentu i Podsekretarz Stanu. W latach 2007–2013 Szef Agencji Bezpieczeństwa Wewnętrznego. Następnie, w latach 2013–2015, Doradca Ministra Obrony Narodowej ds. cyberbezpieczeństwa oraz Dyrektor Narodowego Centrum Kryptologii. Od 2023 r. Dyrektor w MSWiA. Obecnie Pełnomocnik MSWiA ds. organizacji Systemu Bezpiecznej łączności Państwowej.
Odznaczony m.in. Złotym Krzyżem Zasługi (1993), Brązowym Medalem „Za zasługi dla obronności kraju" (1999), Krzyżem Wolności i Solidarności (2012), Krzyżem Komandorskim Orderu Odrodzenia Polski (2013), Odznaką Honorową im. gen. Roweckiego „Grota" (2013).