Analiza KBN

Nr 9 (104) / 2022 17 marca 2022 r.

Czy Polska potrzebuje szóstej służby specjalnej? O pomyśle utworzenia Agencji Cyberbezpieczeństwa

Arkadiusz Nyzio

Dwie głośne w ostatnich miesiącach afery doprowadziły do wzrostu zainteresowania tematem cyberbezpieczeństwa nad Wisłą. Zaowocowały także szybkimi zmianami prawa przeforsowanymi przez rząd. Konkurencyjne propozycje postanowiła złożyć opozycyjna lewica. Autorzy projektu ustawy o Agencji Cyberbezpieczeństwa postulują utworzenie nowej służby specjalnej, która w niektórych sprawach miałaby zastąpić Agencję Bezpieczeństwa Wewnętrznego, a w innych – pełnomocnika rządu do spraw cyberbezpieczeństwa. Pozycja systemowa agencji, jej zadania, kompetencje i struktura zostały opisane i uzasadnione w sposób szczątkowy lub wadliwy. Nawet podzielając niektóre diagnozy projektodawców, trudno przyznać im rację, że proponowana ustawa przyczyniłaby się do wzmocnienia systemu cyberbezpieczeństwa.

Najważniejsze wnioski:

1. Wątpliwy jest sam pomysł tworzenia kolejnej (szóstej) polskiej służby specjalnej. Ich liczba już w tym momencie jest zbyt duża i należy raczej zastanawiać się nad integracją ogniw systemu bezpieczeństwa.
2. Projektodawcy deklarują, że zamierzają rozwiązać problem koordynacji w obszarze cyberbezpieczeństwa, ale nie tłumaczą, z czego wynika ich diagnoza, że taki problem w ogóle istnieje. Poza tym to właśnie nadmierna fragmentaryzacja systemu bezpieczeństwa, którą

realizacja projektu jeszcze by pogłębiła, jest jedną z przeszkód w prowadzeniu skutecznej koordynacji.

3. Nie jest jasne, jakie systemowe funkcje miałaby pełnić Agencja Cyberbezpieczeństwa. Jej proponowane zadania nie pokrywają się z jej postulowanymi kompetencjami.
4. Czynności, które miałaby wykonywać Agencja Cyberbezpieczeństwa, nie zostały dookreślone. Pozostawienie w sferze domysłów odpowiedzi na pytania o zakres przedmiotowy czynności operacyjno-rozpoznawczych (inwigilacja) i dochodzeniowo-śledczych (ściganie sprawców przestępstw) jest niedopuszczalne. Proponowane przepisy są nie tylko niespójne wewnętrznie, ale też niezgodne z konstytucją.
5. Nie przedstawiono argumentów uzasadniających budowę nowej instytucji na bazie części struktury Agencji Bezpieczeństwa Wewnętrznego. Zadanie ochrony krytycznej infrastruktury teleinformatycznej powinna realizować służba odpowiedzialna za problematykę kontrwywiadowczą i antyterrorystyczną.
6. Pomysły dotyczące Krajowego Systemu Cyberbezpieczeństwa nie odnoszą się do żadnego z najważniejszych deficytów w jego funkcjonowaniu. Nie jest prawdą, że w systemie brakuje podmiotów wiodących, co zdają się sugerować projektodawcy. Zostały one wyodrębnione, a relacje pomiędzy nimi są dość wyczerpująco opisane.
7. Wprowadzenie do Krajowego Systemu Cyberbezpieczeństwa jeszcze jednego (trzeciego) podmiotu o uprawnieniach koordynacyjnych doprowadziłoby do sporów kompetencyjnych. Kto koordynować będzie samych koordynatorów?
8. Cele projektodawców można osiągnąć bez powoływania nowej służby specjalnej, drogą nowelizacji przepisów obowiązujących i zwiększenia budżetu właściwych instytucji. Ich infrastrukturalna i kadrowa rozbudowa byłaby rozwiązaniem prostszym, czytelniejszym w sensie systemowym i zdecydowanie tańszym. Działalność profilaktyczna i informacyjna (w tym szeroko zakrojony system szkoleń) może być prowadzona przez instytucje już istniejące, w tym przez urzędy cywilne.

1. Tło polityczno-prawne

W dniu 4 czerwca 2021 r. na komunikatorze internetowym Telegram zaczęto publikować korespondencję elektroniczną pochodzącą z prywatnej skrzynki Michała Dworczyka, posła Prawa i Sprawiedliwości, ministra bez teki i pełnomocnika rządu ds. programu szczepień przeciwko koronawirusowi. Proceder trwa do dzisiaj, wykorzystywane są w nim różne platformy. Nie wiadomo, czy wszystkie maile są prawdziwe (autentyczność części z nich potwierdzili dziennikarze), jak dotąd służbom nie udało się też ustalić, kto stoi za wyciekiem. Rząd nie komentuje sprawy. Afera, nazywana w mediach „Dworczyk leaks", skłoniła polityków do refleksji nad bezpieczeństwem komunikacji internetowej i odpornością państwa na komputerowe ataki i prowokacje.

Do zainteresowania tą problematyką przyczyniła się też tzw. afera Pegasusa, dotycząca oprogramowania szpiegowskiego, po które miały sięgać polskie służby. Pierwsze informacje wiążące aplikację z Polską pojawiły się w raporcie Citizen Lab z września 2018 r., ale temat stał się szerzej znany dopiero na początku 2022 r. Niedawno poświęciłem mu odrębny tekst.

Cyberbezpieczeństwo stało się jednym z najszerzej komentowanych tematów i pierwszoplanowym przedmiotem kontrowersji. Należało więc spodziewać się przygotowanych *ad hoc* propozycji nowelizacji prawa.

27 lipca 2021 r. Mateusz Morawiecki (premier i minister właściwy do spraw informatyzacji), Mariusz Kamiński (minister spraw wewnętrznych i administracji oraz koordynator służb specjalnych) i Janusz Cieszyński (pełnomocnik rządu do spraw cyberbezpieczeństwa) ogłosili pomysł utworzenia nowej struktury centralnej w ramach Policji – Centralnego Biura Zwalczania Cyberprzestępczości (CBZC). Rządowy projekt ustawy o zmianie ustawy o Policji i niektórych innych ustaw w związku z powołaniem CBZC otrzymał numer druku 12 listopada 2021 r.

Tego samego dnia do Sejmu trafił również rządowy projekt ustawy o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, nowelizującej szereg ustaw, na czele z ustawą z 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (KSC). Najważniejszą wprowadzoną zmianą było powołanie do życia Fundusz Cyberbezpieczeństwa.

Oba projekty zostały przyjęte w grudniu 2021 r. Policyjne CBZC zaczęło działać 12 stycznia 2022 r. Wypłata pierwszych świadczeń z Funduszu Cyberbezpieczeństwa rozpoczęła się 1 marca tego roku.

Wcześniej, 8 października 2021 r., nadano numer druku poselskiemu projektowi ustawy o Agencji Cyberbezpieczeństwa (AC), opisującemu zadania, kompetencje i strukturę zupełnie nowej instytucji bezpieczeństwa Polski. Złożyli go politycy reprezentujący Koalicyjny Klub Poselski Lewicy (Nowa Lewica, Razem) i Koło Parlamentarne PPS.

Tak o inicjatywie mówił Krzysztof Gawkowski, przewodniczący Koalicyjnego Klubu Poselskiego Lewicy (Nowa Lewica, Razem) i jeden z sygnatariuszy projektu: „To projekt pokazujący, jak można myśleć w Polsce o kwestiach cyberbezpieczeństwa. Skupia się na polityce prewencyjnej, a nie opresyjnej. Kiedy będą trwały rozmowy o projekcie PiS-u, którego jeszcze nie ma, wtedy te dwa akty powinny być procedowane razem i będzie szansa, że część z naszych przepisów wejdzie w życie". Mówiąc o projekcie PiS-u, miał na myśli wspomniany powyżej rządowy projekt ustawy tworzącej Fundusz Cyberbezpieczeństwa. Punktem wyjścia było przekonanie, że instytucje związane z cyberbezpieczeństwem są zanadto rozproszone. „Mamy w polskim systemie cyberbezpieczeństwa rozbite kompetencje w tej kwestii w wielu różnych miejscach i brak jest komunikacji między służbami. One są dobre – nie twierdzę, że CERT GOV i ABW nie działa dobrze – jednak jest zbyt wiele miejsc, w którym toczą się różnego rodzaju prace" – tłumaczył poseł Gawkowski. Dodał również: „Wierzę, że jeśli PiS nie powoła teraz nowej służby, to w przyszłości rządowi opozycji się to uda". Dodajmy, że Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL (*Computer Emergency Response Team*), o którym wspomniał Gawkowski, w momencie wypowiadania przez niego tych słów nie istniał od ponad trzech lat.

Projekt lewicy czekał w Sejmie na swoją kolej przez prawie pięć miesięcy, ale wreszcie 23 lutego br. został skierowany do pierwszego czytania. Nie wiadomo jeszcze, kiedy izba zajmie się jego rozpatrzeniem.

Jest stosunkowo krótki, zawiera tylko 40 artykułów. Towarzyszy mu kilkunastostronicowe uzasadnienie. Przyjęcie ustawy wiązałoby się z nowelizacją zaledwie trzech ustaw: o Agencji Bezpieczeństwa Wewnętrznego (ABW) i Agencji Wywiadu (AW), o zarządzaniu kryzysowym (ZK) oraz o KSC.

Projekt nie doczekał się dotąd omówienia i nie spotkał z większym zainteresowaniem ze strony opinii publicznej. Wyrażony w nim pogląd, że Polska potrzebuje nowej służby nie jest jednak odosobniony. W międzyczasie, 29 listopada 2021 r., Izba Rzeczoznawców opublikowała ekspertyzę autorstwa Jaroslawa Mojsiejuka i Wiesława Paluszyńskiego. Jej autorzy uznali, że w związku z rosnącą liczbą zagrożeń cybernetycznych, Polska musi przeprowadzić szereg reform, a najważniejszą z nich powinno być utworzenie „rządowej Agencji Cyberbezpieczeństwa, wyposażonej w odpowiednie środki, ludzi i kompetencje i działającej równolegle do stale rozwijanych sił zbrojnych". Jeszcze w 2016 r. utworzenie „narodowej agencji cyberbezpieczeństwa" proponował ówczesny prokurator krajowy Bogdan Święczkowski.

2. Status Agencji Cyberbezpieczeństwa

W Europie i na świecie występuje wiele modeli organizacji aparatu cyberbezpieczeństwa. Istnienie samodzielnych instytucji działających na tym odcinku nie jest rozwiązaniem niespotykanym. Istnieją one chociażby w Niemczech, Francji, Włoszech, Czechach czy w Singapurze, ale w żadnym z tych państw nie są zaliczane do służb specjalnych[1]. Są to instytucje uzupełniające działania domyślnych dysponentów tego obszaru, czyli służb specjalnych zajmujących się kontrwywiadem, ochroną infrastruktury krytycznej i zwalczaniem terroryzmu, a nie odrębne służby specjalne. W innym modelu, którego podręcznikowymi przykładami są USA i Zjednoczone Królestwo, a także, w mniejszym stopniu, Kanada, istnieją wyspecjalizowane instytucje o quasi-samodzielnym statusie: posiadają dużą podmiotowość, ale pozostają częścią instytucji macierzystych – służb specjalnych. W Holandii tego rodzaju komórka jest wspólnym przedsięwzięciem dwóch służb: cywilnej i wojskowej. Częstą praktyką jest powstawanie komórek w strukturach wojskowych i służbach policyjnych. O ile obowiązujące obecnie polskie rozwiązania w zakresie cyberbezpieczeństwa należy uznać za nieodbiegające od europejskiej normy, o tyle propozycję projektodawców trudno zestawić z którąkolwiek spośród znanych autorowi konstrukcji.

W art. 1 projektu zabrakło zwyczajowego określenia ogólnej właściwości i systemowej funkcji instytucji, w rodzaju: „Tworzy się Agencję Cyberbezpieczeństwa, zwaną dalej „AC", jako służbę specjalną, właściwą w sprawach…" Takiej definicji nie znajdziemy również w uzasadnieniu projektu. Przekonanie, że pojęcie „cyberbezpieczeństwo" nie wymaga wyjaśnienia, jest złudne. Piętnaście lat temu z podobnego założenia wyszli autorzy projektu ustawy o Centralnym Biurze Antykorupcyjnym (CBA), którzy nie pokusili się o precyzyjne zdefiniowanie pojęcia „korupcja". Wyrok Trybunału Konstytucyjnego (sygn. K 54/07) przesądził o konieczności kompleksowej regulacji w tym zakresie. Trzeba przy tym zauważyć, że ustawa o CBA w pierwotnym kształcie zawierała ogólną definicję obszaru merytorycznego instytucji, a projekt ustawy o AC nie zawiera jej w ogóle.

[1] Odpowiednio: *nachrichtendienste*, *services de renseignement*, *servizi segreti*, *zpravodajské služby*. W Singapurze raczej nie używa się pochodzącego z malajskiego języka narodowego sformułowania *agensi perisikan*. W powszechnym użyciu jest terminologia angielska.

Niedookreślenie w zakresie tytułowego „cyberbezpieczeństwa" jest zapowiedzią dalszych problemów. Pierwsza poważna wątpliwość dotyczy samej istoty AC. Doktryna obfituje w podobne niejasności, ale dotyczą one ujęcia funkcjonalnego. Na przykład badacze zastanawiają się, jak należy interpretować status CBA, Służby Ochrony Państwa czy Biura Nadzoru Wewnętrznego. Na poziomie formalnoprawnym takich wątpliwości nie ma. Prawodawca expressis verbis określił bowiem, które z instytucji bezpieczeństwa mają status służb specjalnych. Katalog ten jest zamknięty i obejmuje pięć podmiotów: Agencję Wywiadu (AW), Agencję Bezpieczeństwa Wewnętrznego (ABW), Służbę Wywiadu Wojskowego (SWW) i Służbę Kontrwywiadu Wojskowego (SKW) oraz wspomniane już CBA. Katalog ten zawarty jest w ustawie o ABW i AW, w art. 11 poświęconym właściwościom Kolegium do spraw Służb Specjalnych, a także w regulaminie Sejmu, w części poświęconej Komisji do spraw Służb Specjalnych (art. 142 ust. 2).

Lektura projektu ustawy o AC skłania do uznania tej instytucji za szóstą służbę specjalną. Nie kryją tego sami projektodawcy, wskazując, że jednym z zadań agencji (art. 4 pkt 7) ma być „reagowanie na incydenty związane z bezpieczeństwem cybernetycznym i współpraca operacyjna z innymi służbami specjalnymi w celu likwidacji zagrożeń". W ustawie pojawia się również Komisja do Spraw Służb Specjalnych (zob. dalej). Projektodawcy zapomnieli jednak o ważnej sprawie: chcąc utworzyć nową służbę specjalną, należy znowelizować art. 11 ustawy o ABW i AW. W rozdziale szóstym projektu, zawierającym zmiany w przepisach obowiązujących, proponują modyfikację kilku przepisów ustawy o ABW i AW, ale akurat nie tego. Bez tej nowelizacji, a także zmiany regulaminu Sejmu, do czego byłaby potrzebna sejmowa inicjatywa uchwałodawcza, proponowane rozwiązanie będzie wadliwe.

Należy również zaznaczyć, że projekt nie przewiduje utworzenia „czystej" służby specjalnej w rozumieniu *intelligence agency* (służba wywiadowcza), czyli ograniczającej się do czynności związanych z pozyskiwaniem, weryfikowaniem, opracowywaniem i dostarczaniem informacji wartościowych z punktu widzenia bezpieczeństwa państwa. AC ma być również organem ścigania, czyli mieć prawo do prowadzenia czynności dochodzeniowo-śledczych. Byłaby to więc trzecia policyjno-informacyjna hybryda w polskim systemie, po ABW i CBA. Ta kwestia zostanie omówiona szerzej w części 2.4. niniejszego opracowania.

W projekcie musi znaleźć się przepis o następującym kształcie: „W granicach zadań, o których mowa w art. (tu numer artykułu zawierającego katalog zadań), funkcjonariusze AC wykonują: (tu katalog typów czynności)". Z obecnego kształtu projektu wynika, że jego autorzy planują przyznanie tej instytucji prawa do wykonywania trzech typów czynności: analityczno-informacyjnych, dochodzeniowo-śledczych i operacyjno-rozpoznawczych. Każdy z nich powinien być wymieniony i opisany w projekcie.

2. Zadania, kompetencje i struktura Agencji Cyberbezpieczeństwa

2.1. Koordynacja i ogólny kształt Krajowego Systemu Cyberbezpieczeństwa

2.1.1. Ogólne uwagi o koordynacji

Projektodawcy planują przyznanie nowej instytucji 12 zadań (art. 4). Uwagę zwraca pkt 1: „koordynacja krajowego systemu cyberbezpieczeństwa". Z jakiegoś powodu częściowo zdublowano ten przepis w pkt 8: „koordynowanie i rozwijanie krajowego systemu cyberbezpieczeństwa".

Pojęcie „koordynacji" ma charakter wieloznaczny, na co zwraca się uwagę w naukach prawnych oraz naukach o polityce i administracji. Przedstawia się je najczęściej w zestawieniu ze „współdziałaniem". To drugie zakłada równą pozycję zaangażowanych podmiotów, natomiast koordynacja jest formą uprawnienia władczego, choć oczywiście nie tak daleko idącą jak kierownictwo. Koordynowane podmioty nie są podporządkowane podmiotowi koordynującemu, nie ma jednak wątpliwości, że posiada on nad nimi częściową zwierzchność. Jej granice i charakter powinny wynikać z przepisów. Jest to specyficzna konstrukcja, ponieważ – pomimo tych częściowych uprawnień władczych – nie wiąże się ona z klasycznym stosunkiem prawnym w prawie administracyjnym, w którym występuje organ nadrzędny i organ podporządkowany. W koordynacji chodzi o harmonizację działań instytucji (podział obowiązków, przezwyciężanie sporów kompetencyjnych), a zatem mowa o relacji przynajmniej trzech podmiotów: koordynującego i przynajmniej dwóch koordynowanych. Taka sytuacja nie ma miejsca w relacji współdziałania – nie występuje podmiot „ponad" instytucjami, które mają ze sobą współpracować.

W prawie służb specjalnych pojęcie „koordynacja" używane jest przede wszystkim w odniesieniu do uprawnień premiera i ministra koordynatora służb specjalnych oraz w odniesieniu do funkcji Kolegium do Spraw Służb Specjalnych. Jest to „organ opiniodawczo-doradczy w sprawach programowania, nadzorowania i koordynowania", a do jego zadań należy wyrażanie opinii w sprawach koordynowania i współdziałania służb specjalnych. Również same służby (ABW[2]) lub ich szefowie (ABW[3], CBA[4]) posiadają szczegółowe uprawnienia koordynacyjne. Aby zrozumieć wagę tego zagadnienia, należy krótko omówić aktualny kształt KSC.

2.1.2. Najważniejsze aspekty ustroju Krajowego Systemu Cyberbezpieczeństwa

Przyjęcie ustawy o KSC wynikało z konieczności transpozycji do prawa krajowego unijnej dyrektywy 2016/1148, nazywanej Dyrektywą Network and Information Systems (NIS), pierwszego prawa UE w zakresie bezpieczeństwa cybernetycznego. Jej celem było ograniczenie luk w cyberbezpieczeństwie całej wspólnoty poprzez stworzenie minimalnych standardów, do których musiałyby stosować się wszystkie państwa członkowskie. Kształtowane dzięki dyrektywie systemy państw członkowskich mają być elementami europejskiego systemu cyberbezpieczeństwa.

Do chwili wejścia w życie ustawy polskie cyberbezpieczeństwo było obszarem niczyim. Zajmowało się nim wiele podmiotów, ale ich wysiłki były nieujednolicone. Brakowało podziału zadań i odpowiedzialności oraz organów dedykowanych. Głównym celem powołania KSC było stworzenie ram prawnych i funkcjonalnych do zbierania informacji o incydentach komputerowych, skuteczne reagowanie na nie i wykształcanie dzięki temu odporności zbiorowej. Trzeba podkreślić, że zamierzeniem prawodawcy nie było stworzenie scentralizowanej struktury. Cyberbezpieczeństwo z definicji jest obszarem obejmującym zarówno administrację publiczną, jak i sektor prywatny. Chodziło nie o usunięcie tego naturalnego rozproszenia podmiotów, tylko o stworzenie czytelnych proce-

[2] Zob. art. 32aa ust. 1 ustawy o ABW i AW (koordynacja funkcjonowania systemu ostrzegania). *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, Dz. U. 2002, nr 74, poz. 676.
[3] Zob. art. 40 ustawy o ABW i AW (koordynacja czynności operacyjno-rozpoznawczych mogących mieć wpływ na bezpieczeństwo państwa).
[4] Zob. art. 29 ust. 2 ustawy o CBA (koordynacja czynności operacyjno-rozpoznawczych i analityczno-informacyjnych mogących mieć wpływ na realizację niektórych zadań CBA). *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*, Dz. U. 2006, nr 104, poz. 708.

dur w zakresie ich koordynacji i współdziałania. Podobnie z odpowiedzialnością za cyberbezpieczeństwo – nie chodziło o skupienie jej w rękach aparatu państwowego, tylko o wyznaczenie zakresów odpowiedzialności różnym typom podmiotów.

W ustawie o KSC określono pięć typów incydentów (krytyczne, poważne, istotne, o podmiocie publicznym i „zwykłe", art. 2) oraz ustanowiono katalog 20 typów podmiotów tworzących system (art. 4)[5] i katalog 9 organów właściwych do spraw cyberbezpieczeństwa (art. 41)[6]. Powstały też trzy krajowe zespoły reagowania na incydenty bezpieczeństwa komputerowego (*Computer Security Incident Response Team*, CSIRT), które odpowiadają za koordynację obsługi zgłoszonych incydentów[7]. Są to:

- CSIRT MON, który działa w ramach Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni – Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni, jednostki organizacyjnej podległej ministrowi obrony narodowej.
- CSIRT NASK, który jest podporządkowany Naukowej i Akademickiej Sieci Komputerowej – Państwowemu Instytutowi Badawczemu, czyli instytucji nadzorowanej przez ministra właściwego do spraw informatyzacji (a więc ministra cyfryzacji).
- CSIRT GOV, który jest prowadzony przez szefa ABW. Zespół jest częścią struktury ABW, a konkretnie Departamentu Bezpieczeństwa Teleinformatycznego (Departamentu I)[8].

Mogą też powstawać sektorowe zespoły cyberbezpieczeństwa. Ich organizowanie przebiega jednak powoli, dopiero w połowie 2020 r. w Komisji Nadzoru Finansowego powstała pierwsza komórka tego rodzaju (CSIRT KNF).

[5] Krajowy system cyberbezpieczeństwa obejmuje: 1) operatorów usług kluczowych (zgodnie z załącznikiem nr 1 do ustawy); 2) dostawców usług cyfrowych (zgodnie z załącznikiem nr 2 do ustawy); 3) CSIRT MON; 4) CSIRT NASK; 5) CSIRT GOV; 6) sektorowe zespoły cyberbezpieczeństwa; 7) większość jednostek sektora finansów publicznych (czyli: organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały; jednostki samorządu terytorialnego oraz ich związki; związki metropolitalne; jednostki budżetowe; samorządowe zakłady budżetowe; agencje wykonawcze; instytucje gospodarki budżetowej; Zakład Ubezpieczeń Społecznych i zarządzane przez niego fundusze oraz Kasę Rolniczego Ubezpieczenia Społecznego i fundusze zarządzane przez Prezesa Kasy Rolniczego Ubezpieczenia Społecznego; Narodowy Fundusz Zdrowia; uczelnie publiczne; Polską Akademię Nauk i tworzone przez nią jednostki organizacyjne); 8) instytuty badawcze; 9) Narodowy Bank Polski; 10) Bank Gospodarstwa Krajowego; 11) Urząd Dozoru Technicznego; 12) Polską Agencję Żeglugi Powietrznej; 13) Polskie Centrum Akredytacji; 14) Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej; 15) spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej; 16) podmioty świadczące usługi z zakresu cyberbezpieczeństwa; 17) organy właściwe do spraw cyberbezpieczeństwa; 18) PKK; 19) pełnomocnika rządu; 20) Kolegium do Spraw Cyberbezpieczeństwa.

[6] Są to: Komisja Nadzoru Finansowego, minister obrony narodowej i ministrowie właściwi do spraw: gospodarki morskiej; gospodarki wodnej; informatyzacji; zdrowia; żeglugi śródlądowej; energii; transportu.

[7] W art. 26 ust. 1 ustawy o KASC w następujący sposób opisano zadania trzech krajowych CSIRT-ów: „współpracują ze sobą, z organami właściwymi do spraw cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji oraz Pełnomocnikiem, zapewniając spójny i kompletny system zarządzania ryzykiem na poziomie krajowym, realizując zadania na rzecz przeciwdziałania zagrożeniom cyberbezpieczeństwa o charakterze ponadsektorowym i transgranicznym, a także zapewniając koordynację obsługi zgłoszonych incydentów".

[8] ABW nie podaje tej informacji wprost, ale też nie ukrywa, że porozumienia z CSIRT NASK podpisuje dyrektor Departamentu I, upoważniony przez szefa agencji. Przed wejściem w życie ustawy o KSC w ramach Departamentu Bezpieczeństwa Teleinformatycznego ABW od 1 lutego 2008 r. działał wspomniany CERT.GOV.PL.

Czuwanie nad spójnością prawną w zakresie cyberbezpieczeństwa to odpowiedzialność Pojedynczego Punktu Kontaktowego (PKK), który działa przy ministrze cyfryzacji. To właśnie PKK ma pełnić „funkcję łącznika", zapewniając współpracę podmiotów odpowiedzialnych za cyberbezpieczeństwo. To polski odpowiednik *single point of contact* (SPOC).

Jak już wspomniano, ministrem cyfryzacji jest obecnie premier. Ministerstwo Cyfryzacji zlikwidowano jesienią 2020 r., włączając ten dział do Kancelarii Prezesa Rady Ministrów (KPRM). Obszarem cyfryzacji zarządza z poziomu KPRM dwójka sekretarzy stanu. Jeden z nich, Janusz Cieszyński, jest pełnomocnikiem rządu do spraw cyberbezpieczeństwa. To funkcja umocowana w ustawie o KSC, odgrywająca w niej wiodącą rolę. Ustawodawca powierzył bowiem pełnomocnikowi „koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa" (art. 60).

W latach 2018–2020 stanowiska ministra cyfryzacji i pełnomocnika zajmowały różne osoby, a ustawa o KSC w ogóle nie przewidywała możliwości powierzenia funkcji pełnomocnika urzędnikowi w randze ministra. Umożliwiła to nowelizacja z 16 kwietnia 2020 r. Wkrótce potem minister cyfryzacji Marek Zagórski objął stanowisko pełnomocnika. Eksperyment przetrwał pół roku, do objęcia przez premiera funkcji ministra cyfryzacji.

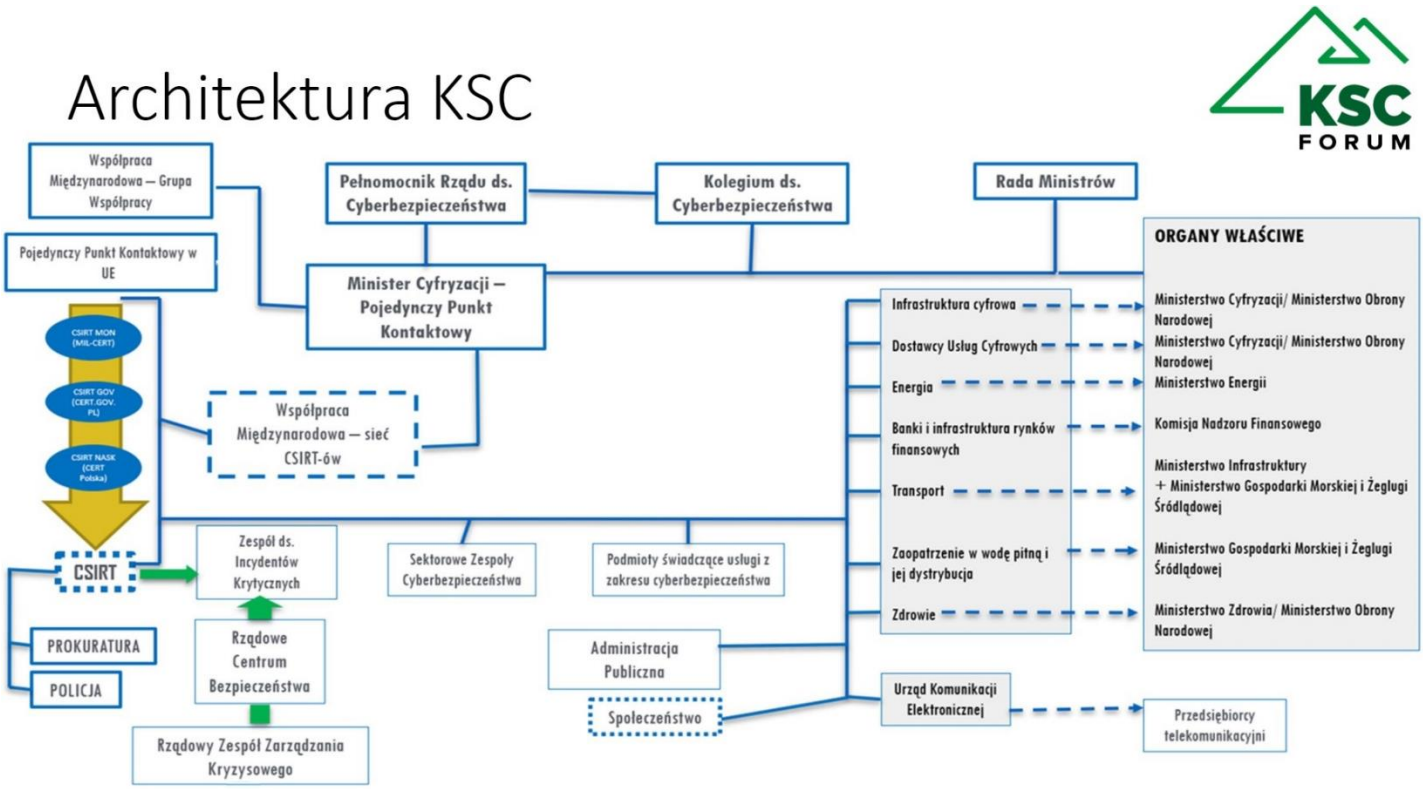
W KPRM istnieją obecnie Departament Cyberbezpieczeństwa (odpowiedzialny za KSC) i Biuro Pełnomocnika Rządu ds. Cyberbezpieczeństwa (odpowiedzialne za obsługę pełnomocnika).

Na podstawie ustawy o KSC przy rządzie działa Kolegium do Spraw Cyberbezpieczeństwa, organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa, działalności w tym zakresie krajowych i sektorowych zespołów cyberbezpieczeństwa oraz organów właściwych do spraw cyberbezpieczeństwa. W jego skład wchodzą m.in. premier (przewodniczący), pełnomocnik i właściwi ministrowie. W odróżnieniu od Kolegium do Spraw Służb Specjalnych, w odniesieniu do zadań Kolegium do Spraw Cyberbezpieczeństwa ustawodawca nie wspomina o wyrażaniu opinii w zakresie koordynacji, a jedynie o takiej możliwości w zakresie współdziałania. W praktyce to właśnie Kolegium do Spraw Cyberbezpieczeństwa jest organem, który ma zapewniać współpracę wszystkich podmiotów zaangażowanych w problematykę cyberbezpieczeństwa.

Uprawnienia koordynacyjne w zakresie cyberbezpieczeństwa ustawodawca przyznał natomiast samemu premierowi. Sformułowano je w art. 67 ust. 1 następująco: „Prezes Rady Ministrów w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa może, na podstawie rekomendacji Kolegium, wydawać wiążące wytyczne dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa, a także żądać informacji i opinii w tym zakresie". Żądanie to może być skierowane do sześciu podmiotów, w tym szefa ABW (w odniesieniu do działalności CSIRT GOV). W art. 67 ust. 2 wyjaśniono, że premier wydaje wiążące wytyczne dla trzech krajowych zespołów CSIRT w zakresie obsługi incydentów krytycznych, wskazuje też, który z nich jest odpowiedzialny za obsługę danego incydentu krytycznego.

Poniżej zamieszczono schemat organizacyjny KSC. Jest to wersja oficjalna, przedstawiona w sierpniu 2019 r. przez Tomasza Wlazia, naczelnika Wydziału KSC w Departamencie Cyberbezpieczeń-

stwa Ministerstwa Cyfryzacji (obecnie w KPRM) na konferencji poświęconej organizowaniu systemu (KSC Forum 2019). Wprawdzie od tamtego czasu ustawa została sześciokrotnie znowelizowana, ale nie były to zmiany o charakterze ustrojowym.



Fundamentami konstrukcji KSC są więc obecnie: pełnomocnik, Kolegium do Spraw Cyberbezpieczeństwa i trzy krajowe CSIRT-y.

2.1.2. *Proponowane zmiany*

Projektodawcy przewidują (art. 6 ust. 1) przyznanie szefowi AC uprawnienia do koordynowania działania niemal wszystkich podmiotów tworzących KSC, z wyjątkiem dwóch: pełnomocnika i kolegium. Zamierzają ponadto znowelizować art. 4 ustawy o KSC, zawierający katalog tworzących system podmiotów. Nie planują jednak modyfikacji listy podmiotów, tylko zamierzają dodać do niego ustęp drugi o następującym brzmieniu: „Szef Agencji Cyberbezpieczeństwa koordynuje współpracę między podmiotami, o których mowa w ust. 1." (art. 37 pkt 2). Przepis ten byłby w kolizji ze wspomnianym art. 6 ust. 1 ustawy o AC. Ich zakres musi być tożsamy. W innym wypadku, po przyjęciu projektu w takim kształcie, z ustawy o KCS wynikałoby, że szef AC koordynuje działanie wszystkich podmiotów tworzących KSC (a więc także pełnomocnika), a z ustawy o AC, że tego nie robi. Pierwsza z tych opcji tworzyłaby konstrukcję osobliwą: szef AC miałby koordynować w zakresie KSC działania innego podmiotu odpowiedzialnego za koordynację KSC.

Tak więc KSC koordynują obecnie dwa podmioty, pomiędzy którymi występuje relacja podległości. Pełnomocnik podlega Radzie Ministrów, jest powoływany i odwoływany przez premiera. To on jest „domyślnym" koordynatorem, o czym świadczy fakt, że jego obowiązki w tym zakresie uregulowano wyczerpująco i wyraźnie wyeksponowano. Natomiast koordynacja premiera ma wyraźnie ogólny charakter.

Szef AC zastąpiłby szefa ABW w kilku miejscach w ustawie o KSC, m.in. w kontekście składu i prac Zespołu do spraw Incydentów Krytycznych oraz informowania o incydentach. Zostałby też członkiem Kolegium do Spraw Cyberbezpieczeństwa. Swojego stałego miejsca nie ma w nim obecnie szef ABW[9], ani szef żadnej innej służby specjalnej lub policyjnej.

Pozycja pełnomocnika zostałaby osłabiona w zakresie jego uprawnień związanych z zarządzaniem kryzysowym. Po pierwsze, chodzi o *Raport o zagrożeniach bezpieczeństwa narodowego*, którego (na podstawie art. 5a ust. 2 ustawy o ZK) przygotowanie koordynują obecnie trzy podmioty: dyrektor Rządowego Centrum Bezpieczeństwa (uprawnienia ogólne), szef ABW (w części dotyczącej zagrożeń o charakterze terrorystycznym, które mogłyby doprowadzić do sytuacji kryzysowej) i pełnomocnik (w części dotyczącej zagrożeń cyberbezpieczeństwa, które mogłyby doprowadzić do sytuacji kryzysowej). Pełnomocnik miałby utracić to uprawnienie na rzecz szefa AC. Po drugie, postulowana jest modyfikacja składu Rządowego Zespołu Zarządzania Kryzysowego, organu opiniodawczo-doradczego Rady Ministrów. W jego posiedzeniach biorą udział (na prawach członka) rozmaite organy, w zależności od potrzeb i przedmiotu posiedzenia. Wśród nich jest pełnomocnik (art. 8 ust. 3 pkt 15 ustawy o ZK), ale projektodawcy mają zamiar zastąpić go szefem AC (art. 36 projektu).

Projektodawcy proponują też zmianę przepisu dotyczącego organizowania pracy Kolegium do Spraw Cyberbezpieczeństwa przez sekretarza kolegium. W tym celu może on obecnie „występować do CSIRT MON, CSIRT GOV, CSIRT NASK, sektorowych zespołów cyberbezpieczeństwa, organów właściwych do spraw cyberbezpieczeństwa oraz organów administracji rządowej o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium". Zamiast tego postulowana jest następująca treść przepisu: „Sekretarz Kolegium organizuje pracę Kolegium i w tym zakresie może występować do Agencji Cyberbezpieczeństwa o przedstawienie informacji niezbędnych w sprawach rozpatrywanych przez Kolegium" (art. 37 pkt 6). Trudno zrozumieć sens tej propozycji. Przecież powstanie AC miałoby wpływ jedynie na CSIRT GOV, a dwa pozostałe zespoły działające na poziomie krajowym funkcjonowałyby w niezmienionej formie. Dlaczego zatem sekretarz musiałby ograniczać się do występowania do szefa AC, nie mogąc zwrócić się do CSIRT MON i CSIRT NASK oraz innych instytucji?

Projektodawcy zamierzają ponadto zmodyfikować wspomniany art. 67 ustawy o KSC. Premier nie mógłby już żądać informacji i opinii w zakresie cyberbezpieczeństwa od sześciu podmiotów (np. ministra właściwego do spraw wewnętrznych w odniesieniu do działalności Policji czy szefa ABW w odniesieniu do działalności CSIRT GOV), tylko od jednego: szefa AC. Nie wydawałby już wiążących wytycznych trzem krajowym CSIRT-om w zakresie obsługi incydentów krytycznych, nie wskazywałby, który z nich jest odpowiedzialny za obsługę danego incydentu krytycznego. Adresatem wytycznych w tym zakresie stałby się szef AC.

„Z punktu widzenia systemu prawnego krajowy system bezpieczeństwa zyska instytucję koordynującą" – reklamowano projekt w uzasadnieniu. Projektodawcy nie tylko przyznają szefowi AC

[9] W skład Kolegium do Spraw Cyberbezpieczeństwa wchodzą: premier (przewodniczący), pełnomocnik i sekretarz oraz członkowie. Są nimi: minister obrony narodowej; ministrowie właściwi do spraw: wewnętrznych, informatyzacji i zagranicznych; szef KPRM-u; szef Biura Bezpieczeństwa Narodowego (jeśli został wyznaczony przez prezydenta) oraz minister koordynator służb specjalnych lub upoważniony przez niego sekretarz lub podsekretarz stanu. Jeśli minister koordynator nie został powołany, to zamiast niego członkiem kolegium jest szef ABW.

zadanie koordynowania KSC, ale wręcz wskazują, że jest to jego podstawowy obowiązek (wspomniany art. 4 ust. 1 projektu). Sęk w tym, że nie postulują odebrania uprawnień koordynacyjnych premierowi (zawartych w art. 67 ust. 1 ustawy o KSC) i pełnomocnikowi (art. 60 ustawy o KSC). A zatem w praktyce koordynatorów byłoby nie dwóch, lecz trzech.

Trzeba jednak zauważyć, że premier i pełnomocnik nie tyle mają „koordynować KSC" (jak szef AC), co koordynować – odpowiednio – działania „administracji rządowej w zakresie cyberbezpieczeństwa" lub działania „w zakresie zapewnienia cyberbezpieczeństwa". Jeśli uznalibyśmy, że nie są to sformułowania o tożsamym zakresie znaczeniowym, to trzeba by dokonać ich gradacji, a także określić jasno, w jakich obszarach i przy użyciu jakich uprawnień ma być realizowana funkcja koordynacyjna tych trzech podmiotów.

Można zgodzić się z ogólnym założeniem, że konstrukcja KSC jest dość zawiła, ale implementacja omawianego projektu w obecnej formie nie przyczyniłaby się do jej uproszczenia. Przeciwnie, doprowadziłaby do zagmatwania relacji pomiędzy organami, a zwłaszcza pomiędzy pełnomocnikiem a szefem AC. Parafrazując znaną sentencję, można zapytać: kto koordynować będzie samych koordynatorów?

2.2. Krytyczna infrastruktura teleinformatyczna

Projektodawcy proponują usunięcie z katalogu zadań ABW rozpoznawania, zapobiegania i wykrywania zagrożeń dotyczących tzw. krytycznej infrastruktury teleinformatycznej (KITI). Odpowiedzialna za to zagadnienie miałaby stać się AC[10]. To stosunkowo nowe zadanie (w sensie prawnym). Przyznano je ABW drogą tzw. ustawy antyterrorystycznej, czyli ustawy z 10 czerwca 2016 r. o działaniach antyterrorystycznych.

Co za tym idzie, projektodawcy proponują usunięcie z ustawy o ABW i AW powiązanych z nim uprawnień, obejmujących:

1. Przeprowadzanie oceny bezpieczeństwa (art. 32a).
2. Wdrażanie, prowadzenie i koordynowanie systemów ostrzegania (art. 32aa).
3. Żądanie udzielenia informacji o budowie, funkcjonowaniu i zasadach eksploatacji systemów teleinformatycznych (art. 32b).

[10] Przepis z art. 5 ust. 1 pkt 2a ustawy o ABW i AW, który miałby zostać przeniesiony do ustawy o AC (art. 4 pkt 2 projektu), wskazuje, że do zadań instytucji należy: „rozpoznawanie, zapobieganie i wykrywanie zagrożeń godzących w bezpieczeństwo, istotnych z punktu widzenia ciągłości funkcjonowania państwa systemów teleinformatycznych organów administracji publicznej lub systemu sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemów teleinformatycznych właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym". Ten ostatni fragment wymaga wyjaśnienia. Rada Ministrów przyjmuje Narodowy Program Ochrony Infrastruktury Krytycznej (art. 5b ust. 1 ustawy o ZK). Określa on m.in: „szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli" (art. 5b ust. 2 pkt 3 ustawy o ZK). Program przygotowuje dyrektor Rządowego Centrum Bezpieczeństwa we współpracy z właściwymi podmiotami (art. 5b ust. 3 ustawy o ZK). On też, działając na podstawie wspomnianych wcześniej szczegółowych kryteriów, we współpracy z ministrami odpowiedzialnymi za 11 systemów infrastruktury krytycznej (art. 3 pkt 2 ustawy o ZK), sporządza „jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy" (art. 5b ust. 7 pkt 1 ustawy o ZK). W wykazie wyróżnia się również „europejską infrastrukturę krytyczną zlokalizowaną na terytorium Rzeczypospolitej Polskiej oraz europejską infrastrukturę krytyczną zlokalizowaną na terytorium innych państw członkowskich Unii Europejskiej, mogącą mieć istotny wpływ na Rzeczpospolitą Polską" (tamże). Wykaz ma niejawny charakter.

4. Zarządzanie blokad dostępności (art. 32c).
5. Prowadzenie rejestru zdarzeń naruszających bezpieczeństwo systemów teleinformatycznych (art. 32d).
6. Wydawanie rekomendacji (art. 32e).

Uprawnienia te przyznano ABW drogą wspomnianej tzw. ustawy antyterrorystycznej. Jak łatwo zauważyć po numeracji artykułów, wyjątkiem jest uprawnienie nr 2, które wprowadzono drogą ustawy o KSC z 2018 r.

Przeprowadzanie oceny bezpieczeństwa (uprawnienie nr 1) miałoby zostać zastąpione kontrolą bezpieczeństwa (art. 19 ust. 1). Podstawowa różnica polegałaby na, jak się wydaje, rozszerzeniu katalogu instytucji, które mogłyby zostać nią objęte. Ocena bezpieczeństwa realizowana przez ABW odnosi się do podmiotów związanych z KITI, w kontekście zdarzeń o charakterze terrorystycznym. Kontrola bezpieczeństwa, którą miałaby realizować AC, byłaby pozbawiona tego kontekstu, dotyczyłaby też wszystkich podmiotów zobowiązanych do współdziałania z AC: 1) instytucji państwowych, 2) organów administracji rządowej i 3) samorządu terytorialnego oraz 4) przedsiębiorców wykorzystujących środki publiczne (art. 7 ust. 1).

Oceny bezpieczeństwa są przeprowadzane co do zasady zgodnie z rocznym planem, opracowywanym w terminie do 30 września roku poprzedzającego. Opracowuje go szef ABW w uzgodnieniu z ministrem cyfryzacji. Natomiast plany przeprowadzania kontroli bezpieczeństwa byłyby opracowywane w terminie do 30 listopada roku poprzedzającego. Przygotowywałby je szef AC w uzgodnieniu z ministrem cyfryzacji.

Po przeprowadzeniu oceny bezpieczeństwa ABW sporządza i przekazuje podmiotowi, którego system podlegał ocenie bezpieczeństwa, raport, który zawiera opis przeprowadzonych czynności i przedstawia wykryte słabości systemu. Z kontrolą bezpieczeństwa byłoby bardzo podobnie, z tym że raportowi towarzyszyłyby też „zalecenia pokontrolne" (art. 20 ust. 1).

Jeżeli w wyniku oceny bezpieczeństwa ABW uzna, że stwierdzona podatność może wystąpić w innych systemach teleinformatycznych, musi niezwłocznie poinformować o tym ministra cyfryzacji. Z AC byłoby bardzo podobnie, ale musiałaby ona poinformować nie ministra cyfryzacji, a premiera (art. 20 ust. 2). To zbyteczny centralizm. Nie ma powodu, aby zakładać, że minister nie poinformuje premiera o szczególnie poważnych przypadkach. Obaj są przecież członkami Kolegium do Spraw Cyberbezpieczeństwa, a nadzwyczajne posiedzenie tego gremium może zostać zwołane na wniosek któregokolwiek z jego członków. Równie zbędne propozycje centralistyczne pojawiają się także w propozycjach dotyczących uprawnień nr 2 i 5.

Zastąpienie sformułowania „niezbędnych druków" sformułowaniem „niezbędnych dokumentów" (art. 21 ust. 2) nie znajduje uzasadnienia, jako że chodzi tu nie o każdy rodzaj dokumentu, tylko właśnie o druki.

W omawianym fragmencie znajdziemy jeden z wielu przykładów niestaranności projektodawców i przejawów przypadkowości projektu. Przepisy dotyczące kontroli bezpieczeństwa AC stworzono kopiując przepisy dotyczące oceny bezpieczeństwa ABW, a następnie wprowadzając w nich drobne zmiany. Redaktorom zabrakło jednak koncentracji, bo pozostawiono sformułowania

„podlegającym tej ocenie" (powinno być: „kontroli") i „podatności ocenianego systemu" (powinno być: „kontrolowanego").

Zwracam też uwagę, że proponowane pojęcie „kontrola bezpieczeństwa" jest niefortunne, jako że w obszarze bezpieczeństwa odnosi się ono do problematyki bezpieczeństwa portów lotniczych. Jest to nie tylko pojęcie używane w doktrynie, ale także obecne w porządku normatywnym, posiadające umocowanie w prawie Unii Europejskiej. Zgodnie z zawartą w nim definicją, kontrola bezpieczeństwa to „stosowanie technicznych lub innych środków w celu identyfikacji lub wykrywania przedmiotów zabronionych". W związku z tym, a także z uwagi na fakt, że proponowane przez projektodawców modyfikacje omawianych przepisów tego nie wymagają, nie widzę sensu w zastępowaniu pojęcia „ocena bezpieczeństwa" pojęciem „kontrola bezpieczeństwa".

Przepisy dotyczące systemu ostrzegania (uprawnienie nr 2) zostałyby przeniesione z ustawy o ABW i AW do ustawy o AC w większości w niezmienionej formie, za wyjątkiem kilku szczegółów. Obecnie ABW uzgadnia z właściwym podmiotem techniczne aspekty uczestnictwa w systemie ostrzegania. Jeśli zawarcie takiego porozumienia nie może dojść do skutku w związku z kwestiami leżącymi po stronie tego podmiotu, szef ABW informuje nadzorcę tego podmiotu lub ministra cyfryzacji. Projektodawcy planują zastąpienie tego ostatniego przez premiera (art. 22 ust. 8). Ponadto, wdrożenie elementów systemu ostrzegania co do zasady następuje zgodnie z rocznym planem wdrożenia, opracowywanym przez szefa ABW w terminie do 30 września roku poprzedzającego. Projektodawcy proponują, aby w odniesieniu do szefa AC był to 30 listopada roku poprzedzającego (art. 22 ust. 2).

Przepisy dotyczące żądania udzielenia informacji (uprawnienie nr 3) zostałyby przeniesione do ustawy o AC generalnie bez zmian, wyjąwszy te o charakterze redakcyjnym. Zwracam jednak uwagę na problem redakcyjny. W art. 23 ust. 1 projektu znalazł się następujący passus: „dotyczącego systemów lub danych, o których mowa w art. 4 pkt 2". Otóż w art. 4 pkt 2 projektu nie ma mowy o danych. Wspomina się o nich natomiast w art. 32a ust. 1 ustawy o ABW i AW, który w kontekście uprawnienia nr 1 był punktem odniesienia dla projektodawców.

Przepisy dotyczące blokady dostępności (uprawnienie nr 4) zostałyby przeniesione do ustawy o AC bez zmian (art. 24).

Przepisy dotyczące rejestru (uprawnienie nr 5) zostałyby przeniesione w niezmienionym kształcie, za wyjątkiem jednej kwestii. Obecnie dane z rejestru są udostępniane ministrowi cyfryzacji, a projektodawcy zamierzają zastąpić go premierem (art. 25 ust. 4).

Wydawanie rekomendacji (uprawnienie nr 6) projektodawcy planują zastąpić wydawaniem zaleceń. Sytuacja związana z tymi przepisami przypomina sprawę uprawniania nr 1. Tutaj również intencją projektodawców zdaje się być analogiczne rozszerzenie podmiotów mających być adresatami tego uprawnienia. Niewykonywanie zaleceń AC byłoby opatrzone nieco szerszą sankcją niż wykonywanie rekomendacji ABW. W przypadku nieuwzględnienia rekomendacji szef ABW występuje do organu sprawującego nadzór nad podmiotem, które je otrzymał, z informacją o tym fakcie lub z wnioskiem o podjęcie działań mających wywołać ich implementację. W przypadku zaleceń AC znaczenie miałby typ podmiotu. Jeśli zaleceń nie wykonywałby podmiot sektora administracji publicznej, to szef AC dysponowałby dokładnie takim samym uprawnieniem, jak szef ABW

w związku z niewykonaniem rekomendacji. Natomiast pozostałe podmioty niewykonujące zaleceń AC podlegałyby karze grzywny (art. 18 ust. 5). Także i w odniesieniu do tego uprawnienia widać niestaranność projektodawców, którzy – kopiując i modyfikując przepisy ustawy o ABW i AW – pozostawili sformułowanie „wpływ rekomendowanych działań" (powinno być: „zalecanych"). Sens propozycji zmiany pojęcia jest niejasny, jako że „zalecenia" i „rekomendacje" to wyrazy bliskoznaczne. Zabieg ten sprawia wrażenie próby zmiany „na siłę".

Warto zauważyć, że realizacja wszystkich wymienionych powyżej uprawnień bezpośrednio lub pośrednio wiąże się z problematyką antyterrorystyczną i kontrwywiadowczą oraz z funkcją krajowej władzy bezpieczeństwa. AC miałaby przejąć zadanie ochrony KITI, nie zajmując się żadnym z wymienionych obszarów. Musiałaby więc zdublować odpowiedzialne za nie struktury lub realizować swoje obowiązki w bliskiej współpracy z ABW.

2.3. Czynności operacyjno-rozpoznawcze

O czynnościach operacyjno-rozpoznawczych AC wiadomo na razie tyle, że prawdopodobnie agencja miałaby je realizować. Stałaby się dwunastą polską instytucja bezpieczeństwa wyposażoną w tego rodzaju uprawnienie. Rozwiązanie to należy uznać za zbędne, projektodawcy nie podali zresztą ani jednego argumentu na jego poparcie. Dysponujące tym uprawnieniem instytucje już teraz obejmują każdy obszar merytoryczny przestępstw i zagrożeń.

Nie chodzi tylko o samą ideę. Równie poważne mankamenty widoczne są także na poziomie wykonania. Projektodawcy nie wspominają ani o przetwarzaniu tzw. metadanych (m.in. bilingi i dane geolokalizacyjne)[11], ani o kontroli operacyjnej (m.in. podsłuchy), ani o pracy z agenturą. Czynnościom operacyjno-rozpoznawczym nie poświęcono wyraźnie wyodrębnionej części ustawy, jak w przypadku każdej innej instytucji uprawnionej do ich prowadzenia, a ich obecności trzeba się w zasadzie domyślać. W projekcie jest mowa o „współpracy operacyjnej z innymi służbami specjalnymi" (art. 4 pkt 7), a w innym, że uzyskane informacje niejawne mogą być przekazywane „jedynie funkcjonariuszom AC prowadzącym w danym postępowaniu czynności operacyjno-rozpoznawcze" (art. 23 ust. 2). Czynności operacyjno-rozpoznawcze muszą posiadać precyzyjne unormowanie. W pierwszej kolejności dotyczy to ich szczególnie dotkliwej dla praw i wolności obywatelskich formy – kontroli operacyjnej. Jej prowadzenie musi być powiązane z zamkniętym katalogiem przestępstw i klauzulą subsydiarności. Sytuacja, w której należy domyślać się, jakimi uprawnieniami dysponuje służba specjalna, jest niedopuszczalna w świetle ustawy zasadniczej.

Można by sądzić, że pojawiające się w projekcie pojęcie „operacyjne" używane jest w innym rozumieniu lub że pojawia się tam przypadkowo, ale w uzasadnieniu projektu stwierdzono: „Propozycja powołania Agencji Cyberbezpieczeństwa jest zatem wyjściem naprzeciw nowoczesnym trendom technologicznym. To stworzenie instytucji realizującej zadania edukacyjne, prewencyjne i operacyjne".

[11] Są to dane niestanowiące treści, pochodzące z przekazu telekomunikacyjnego, przesyłki pocztowej albo przekazu w ramach usługi świadczonej drogą elektroniczną.

2.4. Uprawnienia policyjne i procesowe

Jak wspomniano, projektodawcy przewidują przyznanie AC statusu organu ściągania. Uregulowanie tej kompetencji jest równie szczątkowe (czy właściwie nieistniejące) jak to dotyczące czynności operacyjno-rozpoznawczych. „Ściganie sprawców" pojawia się w projekcie trzykrotnie: w kontekście systemu ostrzegania (art. 22 ust. 1), żądania udzielenia informacji o budowie, funkcjonowaniu i zasadach eksploatacji systemów teleinformatycznych (art. 23 ust. 1) oraz blokady dostępności (art. 24 ust. 1). Za każdym razem kontekstem są przestępstwa o charakterze terrorystycznym.

Nie wspomina się jednak o postępowaniu przygotowawczym, nie pada w ogóle pojęcie „czynności dochodzeniowo-śledcze" czy „postępowanie przygotowawcze", brak jest wzmianki o wykonywaniu czynności na polecenie sądu lub prokuratora. Wśród zadań instytucji nie znalazła się zwyczajowa konstrukcja związana z funkcją ścigania: „rozpoznawanie, zapobieganie i wykrywanie przestępstw (tu katalog) oraz ściganie ich sprawców". Nawet więcej: w zadaniach AC w ogóle nie wspomina się nie tylko o jakichkolwiek przestępstwach i ich ściganiu, ale także o terroryzmie.

Nie można wykluczyć, że projektodawcy w ogóle nie planują przyznania AC takiego uprawnienia. Być może po prostu skopiowali fragmenty ustawy o ABW i AW, nie zauważając, że stwierdzenie „ściganie sprawców" pociągania za sobą daleko idące konsekwencje.

Jeśli AC miałaby ścigać sprawców określonych przestępstw, to musiałaby dysponować własnym pionem prawnym (śledczym, postępowania karnego), a także szeregiem uprawnień policyjnych, np. możliwością legitymowania osób w celu ustalenia ich tożsamości czy zatrzymywania ludzi. Takich uprawnień dla AC jednak projektodawcy nie przewidują. Ponadto, gdyby nawet je przewidzieli, to funkcjonariusze AC nie mogliby ich realizować bez możliwości używania przymusu. Projektodawcy w ogóle się do tego zagadnienia nie odnoszą i nie postulują nowelizacji ustawy z 24 maja 2013 r. o środkach przymusu bezpośredniego i broni palnej. Tego rodzaju uprawnienie posiadają wszystkie służby specjalne i policyjne, a także szereg innych instytucji, m.in. strażnicy gminni czy strażnicy Państwowej Straży Rybackiej (w sumie 20 podmiotów). Trudno wyobrazić sobie, aby miała ich nie mieć służba specjalna.

2.5. Profilaktyka i informowanie

Cztery spośród proponowanych zadań instytucji ma charakter bardzo „miękki", szeroki i niedookreślony. Mowa o: prowadzeniu „działań prewencyjno-edukacyjnych związanych z cyberbezpieczeństwem w sektorze publicznym i prywatnym" (art. 4 pkt 3); budowaniu „świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa" (art. 4 pkt 4); wspieraniu „jednostek nauki i szkolnictwa wyższego w zakresie bezpieczeństwa w cyberprzestrzeni" (art. 4 pkt 9); monitorowaniu „rozwoju nowoczesnych technologii i ich wpływu na życie człowieka" (art. 4 pkt 10). Zawieszono je niejako w próżni. Przykładowo, z projektu w żaden sposób nie wynika, jak (a przede wszystkim – po co?) służba specjalna miałaby monitorować wpływ technologii na życie człowieka.

Projektodawcy zamierzają wprowadzić szereg rozwiązań z zakresu profilaktyki cyberbezpieczeństwa. Chcą powierzyć AC obowiązek czuwania nad realizacją wdrażania dobrych praktyk przez wymienione w części 2.2. niniejszego opracowania cztery typy podmiotów zobowiązanych do

współdziałania z agencją. Obejmowałoby to cztery obowiązki: 1) „wdrażania zaleceń Szefa AC dotyczących podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności; 2) „stosowania oprogramowania spełniającego standardy AC"; 3) „umożliwienia przeprowadzenia kontroli bezpieczeństwa systemów teleinformatycznych, zabezpieczeń danych i sprzętu elektronicznego"; 4) umożliwienia pracownikom uczestniczenia w szkoleniu z zakresu cyberbezpieczeństwa (art. 7 ust. 2). Szkolenia dla pracowników czterech wspomnianych powyżej typów podmiotów byłyby bezpłatne, ale na zasadzie (niewielkiej) odpłatności byłyby też dostępne dla wszystkich zainteresowanych. Wpływy z opłaty byłyby dochodem AC (art. 16).

W przypadku instytucji sektora administracji publicznej, niewykonanie obowiązków nr 2, 3 i 4 byłoby podstawą do wystąpienia przez Szefa AC do sprawującego nad nim nadzór organu z informacją o niewykonaniu obowiązków lub z wnioskiem o podjęcie działań mających na celu ich wykonanie. Inne podmioty podlegałyby karze grzywny (art. 7 ust. 3).

Aspektem działań profilaktycznych jest z pewnością obowiązek informowania opinii publicznej o stanie cyberbezpieczeństwa. Projektodawcy przewidują jego pięć (?) wymiarów.

Po pierwsze, szef AC miałby publikować „standardy oprogramowania i zarządzania bezpieczeństwem informacji". Miałyby one powstawać na podstawie „norm międzynarodowych" i „bieżących zaleceń" szefa AC dotyczących „podniesienia poziomu bezpieczeństwa systemów teleinformatycznych w celu zapewnienia ich integralności, poufności, rozliczalności i dostępności" (art. 17).

Po drugie, szef AC miałby obowiązek przedstawiania rocznej informacji o stanie cyberbezpieczeństwa państwa (art. 11 ust. 1 pkt 4 projektu, por. „po dziesiąte" w części 3. niniejszego opracowania). To rozwiązanie pożyteczne, zwłaszcza w świetle widocznej w ostatnich latach dużej wstrzemięźliwości polskich służb specjalnych do prowadzenia komunikacji społecznej. ABW zaprzestała publikowania corocznych „raportów z działalności", nie posiada już swojego rzecznika prasowego (podobnie jak CBA). Wszystkie służby specjalne podchodzą niechętnie do udostępniania informacji publicznych, nawet w błahych sprawach zasłaniając się bezpieczeństwem lub obronnością państwa. W tej sytuacji wprowadzenie ustawowego obowiązku przedstawiania informacji o bezpieczeństwie cybernetycznym państwa jest rozwiązaniem pożądanym. Wymaga jednak doprecyzowania w zakresie przedmiotowym i czasowym: komu szef AC miałby przedstawiać informacje, jakie byłyby to informacje (warunki brzegowe) i w jakim terminie? Można w tym zakresie sięgnąć na przykład po przepisy ustawy z 28 stycznia 2016 r. Prawo o prokuraturze (art. 11).

Trzeba przy tym zaznaczyć, że już dzisiaj, pomimo braku ustawowego obowiązku, publikowane są roczne *Raporty o stanie bezpieczeństwa cyberprzestrzeni RP*. W latach 2011–2018 przygotowywał je CERT.GOV.PL działający w strukturze ABW, a od 2019 r. zajmuje się tym CSIRT GOV. Do momentu zamknięcia tego tekstu opublikowano 11 rocznych raportów.

Po trzecie, szef AC przekazywałby premierowi informację o bieżącym stanie cyberbezpieczeństwa. Szczegóły w tym zakresie ustaliłby premier w drodze zarządzenia (art. 15).

Po czwarte, szef AC przedstawiałby Komisji do Spraw Służb Specjalnych i właściwej komisji sejmowej do spraw cyfryzacji roczną informację o stanie cyberbezpieczeństwa państwa (art. 26). Nie

wiadomo, czy projektodawcy mają tu na myśli ten sam obowiązek informowania, o którym wspomniano powyżej w punkcie „po drugie" (art. 11 ust. 1 pkt 4). Nawiasem mówiąc, fakt, że w artykule zawierającym tylko jeden przepis umieszczono numer ustępu, jest jeszcze jednym potwierdzeniem, że projekt powstawał w pośpiechu, że nie został przemyślany i że nie poddano go ocenie eksperckiej.

Po piąte, szef AC miałby obowiązek cotygodniowego publikowania na stronie internetowej instytucji raportu o stanie cyberbezpieczeństwa, zawierającego m.in. „ogólną ocenę bezpieczeństwa cyfrowego", „komunikaty o ostrzeżeniach przed atakami" i „bieżące zalecenia w zakresie cyberbezpieczeństwa" (art. 14). Trzeba zaznaczyć, że już teraz, pomimo braku ustawowego obowiązku, CSIRT GOV prowadzi tego rodzaju działalność. Obecnie dostępna jest datowana na 17 grudnia 2021 r. informacja o incydencie Log4Shell, czyli krytycznej luce w zabezpieczeniach popularnej biblioteki Apache Log4j. Powstała w oparciu o prace wszystkich trzech CSIRT-ów. Tak jak w przypadku sprawy z punktu „po drugie", należy ocenić pozytywnie propozycję uregulowania obowiązków informacyjnych w ustawie.

Jeśli celem instytucji ma być prowadzenie na potrzeby państwa prac eksperckich w zakresie cyberbezpieczeństwa, jak wynika z katalogu jej zadań, to w projekcie należy zawrzeć informację o prowadzonych przez jej funkcjonariuszy czynnościach analityczno-informacyjnych („uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla…").

2.6. Pragmatyka

Projekt zawiera szczątkowe przepisy pragmatyczne, ujęte w rozdziale czwartym, zatytułowanym „Pracownicy i funkcjonariusze Agencji Cyberbezpieczeństwa". To zaledwie pięć artykułów (art. 27–31), a na dodatek ostatni z nich wskazuje: „W zakresie nieregulowanym niniejszą ustawą funkcjonariuszom AC przysługują uprawnienia funkcjonariuszy, o których mowa w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu". Można rozumieć to dwojako – i w obu wariantach jest to rozwiązanie wadliwe.

W wersji pierwszej projektodawcy mieli na myśli jedynie przepisy pragmatyczne. Czyli ograniczyli się do przedstawienia różnic w pragmatyce, wskazując, że – poza wskazanymi odstępstwami – do funkcjonariuszy AC odnoszą się przepisy pragmatyczne zawarte w ustawie o ABW i AW. To rozwiązanie niestosowane w polskich służbach policyjnych i specjalnych. Ustawa o Straży Granicznej nie przekierowuje pograniczników do ustawy o Policji, a ustawa o CBA nie odsyła w tym zakresie do ustawy o ABW i AW. Wyjątkami są ustawa o Żandarmerii Wojskowej oraz ustawa o SKW i SWW, w których zawarto przepisy pragmatyczne, ale jednocześnie umieszczono odwołanie do ustawy z 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych („w sprawach nieuregulowanych w ustawie stosuje się…"). Wynika to jednak ze specyficznego statusu służb wojskowych. Służby cywilne mają własną pragmatykę dołączoną do ich ustaw kompetencyjnych i jeśli intencją projektodawcy jest przyjąć rozwiązania zawarte w ustawie o ABW i AW jako modelowe, to powinny one zostać *mutatis mutandis* przeniesione do ustawy o AC. W wersji minimalnej należy wskazać, które konkretnie artykuły pragmatyczne ustawy o ABW i AW mają zastosowanie dla funkcjonariuszy AC.

W interpretacji drugiej przytoczone sformułowanie może prowadzić do problemów podobnych do tych, jakie w latach 90. wynikały z braku kompleksowego uregulowania zadań i kompetencji

wojskowych służb specjalnych. Nie przyjęto poświęconej im odrębnie ustawy, a ich umocowanie miało charakter lakonicznych wzmianek w innych normatywach. Wśród nich była ustawa z 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (UOP), w której wskazano, że przewidziane dla tej instytucji zadania „wykonują także służby wywiadu i kontrwywiadu podległe Ministrowi Obrony Narodowej na zasadach i w trybie określonych w odrębnych przypisach". Przepis ten uchylono dopiero w 1995 r. Drugim problematycznym normatywem była ustawa z 21 listopada 1967 r. o powszechnym obowiązku obrony RP, w której wskazano: „Obowiązki i uprawnienia związane z wykonywaniem czynności służbowych przez funkcjonariuszy Urzędu Ochrony Państwa dotyczą odpowiednio żołnierzy Wojskowych Służb Informacyjnych w zakresie wykonywanych przez nich zadań, a uprawnienia Urzędu Ochrony Państwa dotyczą odpowiednio Wojskowych Służb Informacyjnych". Taki stan prawny doprowadził do poważnych wątpliwości i kontrowersji dotyczących granic kompetencyjnych wojskowych służb specjalnych, przeciętych wreszcie orzeczeniem TK z 1996 r. (sygn. W 12/94). Raz jeszcze należy podkreślić, że zadania i kompetencje służb specjalnych, zwłaszcza te mające wpływ na prawa i wolności obywatelskie, nie mogą być przedmiotem niejasności, nie powinny być też pozostawione do wyinterpretowania. Powinny explicite wynikać z ustawy.

2.7. Struktura

Jedyną częścią struktury AC, o które wspomniano w projekcie, jest CSIRT GOV, który zostałby przeniesiony z ABW. Stałoby się to w terminie 6 miesięcy od dnia wejścia w życie ustawy (art. 13 ust. 1; art. 38). W AC zatrudnieni byliby zarówno pracownicy, jak i funkcjonariusze. Z uwagi na zadania instytucji jest to niewątpliwie rozwiązanie słuszne, zwraca jednak uwagę przyjęcie przez projektodawców zbyt sztywnego podejścia. Funkcjonariusze pełniliby służbę w ramach CSIRT GOV, a w pozostałych jednostkach zatrudniano by na etatach cywilnych (art. 27). Przyjęcie tego rozwiązania niechybnie generowałoby problemy organizacyjne. Po pierwsze dlatego, że z pewnością w innych komórkach zaszłaby potrzeba zatrudnienia osób mogących prowadzić czynności wymagające statusu funkcjonariusza. Po drugie, już teraz CSIRT GOV zatrudnia na stanowiskach cywilnych (np. specjalista ds. bezpieczeństwa IT). Założenie, że wszyscy zatrudnieni tam cywile zajmujący się siecią TCP/IP, elektroniką, telekomunikacją, Unixem czy Linuxem, musieliby zostać funkcjonariuszami, jest nielogiczne i przeciwskuteczne. Wydaje się, że projektodawcy błędnie postrzegają CSIRT GOV jako typową mundurową strukturę służby specjalnej.

Być może projektodawcy mają na myśli to, że funkcjonariusze służyliby wyłącznie w CSIRT GOV, a nie że CSIRT GOV zatrudniałby wyłącznie funkcjonariuszy. W przepisach przejściowych i końcowych projektodawcy wskazali bowiem: „pracownicy i funkcjonariusze ABW zatrudnieni w ramach CSIRT GOV, po upływie terminu (…) stają się pracownikami i funkcjonariuszami AC" (art. 38 ust. 3). W odniesieniu do takich funkcjonariuszy stosowano by przepisy pragmatyczne z ustawy o ABW i AW.

Z projektu nie dowiadujemy się niczego o strukturach terenowych AC. Trudno powiedzieć, czy projektodawcy nie przewidują ich istnienia (czyli że istnieć ma tylko struktura centralna, jak w AW i SWW), czy też kwestia ta została pozostawiona do rozstrzygnięcia na dalszych etapach procesu legislacyjnego.

3. Pozycja systemowa szefostwa Agencji Cyberbezpieczeństwa

Na czele AC miałby stanąć szef AC, powoływany przez premiera, po zasięgnięciu opinii sejmowej Komisji do Spraw Służb Specjalnych oraz właściwej komisji sejmowej do spraw cyfryzacji (art. 8 ust. 2). Obecnie jest to Komisja Cyfryzacji, Innowacyjności i Nowoczesnych Technologii.

Po pierwsze, projektodawcy nie przewidują przyznania szefowi AC statusu centralnego organu administracji rządowej. Jest to sprzeczne z dotychczasową praktyką, kompletnie niezrozumiałe i pozostawione bez jakiegokolwiek uzasadnienia. Przyjęcie tego rozwiązania sprawiłoby, że szef jednej z sześciu służb specjalnych miałby pozycję wyraźnie słabszą, niż szefowie pozostałych pięciu. Obecnie w tym względzie panuje względna[12] równowaga. Proponowane rozwiązanie jest nie tylko wątpliwe pod kątem prawno-systemowym, ale także przeciwskuteczne politycznie. Projektodawcy przewidują (art. 6. ust. 2), że AC w ramach swojej działalności będzie współpracować z innymi podmiotami, w tym ze wszystkimi służbami policyjnymi i specjalnymi. To oczywiste. Trzeba jednak zauważyć, że szef AC występowałby wobec szefów ABW, AW, SKW i SWW ze słabszej pozycji. Również szefowie Policji, Straży Granicznej czy Służby Ochrony Państwa są centralnymi organami. Z pozycji silniejszego występowałby jedynie wobec komendanta głównego Żandarmerii Wojskowej. To przepis na pogłębienie podziałów w i tak już wystarczająco zwaśnionym świecie służb.

Po drugie, projektodawcy nie wskazali, komu miałby podlegać szef AC. Z samego powoływania przez premiera nie wynika stosunek podległości. Szefów SKW i SWW powołuje premier, ale – z wyjątkiem zastrzeżonych dla niego uprawnień – podlegają one ministrowi obrony narodowej. Z faktu, że żaden minister nie jest przewidywany w procedurze powoływania jako wnioskodawca, należy wnosić, że projektodawcom chodzi o podległość szefowi rządu, wprost musi to jednak wynikać z ustawy.

Po trzecie, projektodawcy nie posłużyli się pojęciem „powołuje i odwołuje" stosowanym w analogicznych aktach normatywnych, co jest błędem w sztuce legislacyjnej (por. „po czwarte").

Po czwarte, projektodawcy postulują dopisanie szefa AC do grona uczestników posiedzeń rządowego Kolegium do Spraw Służb Specjalnych (art. 35 pkt 2), ale nie uwzględniają zasięgnięcia opinii tego organu w procedurze jego powołania, co jest właściwe dla wszystkich polskich służb specjalnych. Proponują natomiast nowelizację ustawy o ABW i AW, polegającą na dopisaniu szefa AC do katalogu organów, w sprawie powołania i odwołania których kolegium wyraża opinię (art. 35 pkt 2). To wadliwe rozwiązanie: kształt art. 8 ust. 2 ustawy o AC powinien być tożsamy z art. 12 ust. 1 pkt 1 ustawy o ABW i AW[13]. Nie może być bowiem tak, iż więcej o powoływaniu i odwoływaniu szefa AC wynika z ustawy o ABW i AW niż z ustawy o AC.

Po piąte, zasięganie opinii właściwej komisji sejmowej do spraw cyfryzacji jest dopuszczalne, ale nielogicznie w świetle dotychczasowej praktyki. Na podobnej, „branżowej" zasadzie można by argumentować, że opinię w sprawie szefa ABW powinna wydawać Komisja Administracji i Spraw

[12] Wyłomem w niej jest powoływanie szefa CBA na czteroletnią kadencję. Poza tym szefowie SKW i SWW podlegają ministrowi obrony narodowej, z zastrzeżeniem uprawnień premiera lub ministra-koordynatora.

[13] Katalog pięciu służb specjalnych jest też zawarty w art. 5 ust. 3 ustawy o CBA. Nie pada tam wprawdzie sformułowanie „służby specjalne", ale dla celów dobrej legislacji należałoby znowelizować i ten artykuł.

Wewnętrznych (z uwagi na funkcje policyjne) czy Komisja Infrastruktury (z uwagi na ochronę infrastruktury krytycznej), a w sprawie szefa CBA – Komisja Finansów Publicznych (z uwagi na realizowane funkcje kontrolne w zakresie wydatkowania środków publicznych) czy Komisja Gospodarki i Rozwoju (z uwagi na ochronę w interesów ekonomicznych państwa). Skupiając w 1995 r. w Komisji do Spraw Służb Specjalnych całość problematyki służb specjalnych prawodawca jasno wskazał, że pomimo tego, iż wiele spraw dotyczących służb łączy się z właściwościami innych komisji, to właśnie to ciało o specjalnym statusie ma za zadanie prowadzić nad nimi specjalistyczny nadzór i kontrolę. Odrębną sprawą jest to, że w obecnym kształcie systemowym Komisja do Spraw Służb Specjalnych nie jest w stanie skutecznie wywiązywać się z tego obowiązku.

Po szóste, w procedurze powoływanie szefa AC nie uwzględniono prezydenta, co również stanowi nieuzasadnione odejście od dotychczasowej praktyki w zakresie służb specjalnych. Jak już wspomniano, prezydent jest uwzględniony w polityce cyberbezpieczeństwa, mogąc wyznaczyć szefa Biura Bezpieczeństwa Narodowego do zasiadania w rządowym Kolegium do Spraw Cyberbezpieczeństwa. Wyłączanie głowy państwa z tej procedury (jak również z całej ustawy) wydaje się bezcelowe.

Po siódme, zwraca uwagę fakt, że projektodawcy posługują się pojęciem „powołuje zastępcę" (art. 8 ust. 3), a zatem przewidziano istnienie tylko jednego takiego stanowiska. Wszystkie pozostałe ustawy dotyczące służb specjalnych stwarzają możliwość powoływania „zastępców", nie precyzując ich liczby. Być może projektodawcy kierowali się logiką oszczędności, ale w tworzeniu prawa trzeba pamiętać o długim horyzoncie. Jeśli ustawa zostałaby uchwalona, to być może za kilka lat pojawiłaby się konieczność rozbudowy instytucji, a jej szef uznałby za zasadne powołanie drugiego zastępcy. To zresztą logiczne, ponieważ w służbach zazwyczaj jeden z zastępców odpowiada za sprawy operacyjne, a drugi za inne obszary, np. sprawy kwatermistrzowskie. Gdyby pojawiła się taka konieczność, ustawa musiałaby zostać znowelizowana. Prawo powinno być pisane w taki sposób, aby unikać ciągłych nowelizacji o drobnym charakterze.

Po ósme, w art. 8 ust. 4 projektodawcy wprowadzają katalog warunków, które muszą spełniać kandydaci na stanowiska szefa i zastępcy szefa AC (por. „po jedenaste"). Takie katalogi zawarte są we wszystkich ustawach kompetencyjnych dotyczących służb specjalnych. Zawierając sześć (ABW, AW), siedem (CBA) lub osiem (SKW i SWW) pozycji. Projektodawcy przewidują natomiast pięć. Trzy z nich są kopią rozwiązań stosowanych we wszystkich służbach specjalnych: „posiada wyłącznie obywatelstwo polskie", „korzysta z pełni praw publicznych" i „spełnia wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli tajności »ściśle tajne«". Czwarty został przeniesiony z ustaw o ABW i AW oraz SKW i SWW, nie ma go w ustawie o CBA: „daje rękojmię należytego wykonywania zadań". Piąty jest nowością. Projektodawcy proponują ściśle merytoryczne kryterium: „posiada przynajmniej 5- letnie doświadczenie w zakresie cyberbezpieczeństwa". Nie zamierzam z tym polemizować, zwracam jednak uwagę, że ukształtowany w Polsce model nie zakłada (wbrew zamysłom z lat 90.) fachowości ścisłego kierownictwa służby specjalnej. Tym samym trudniej byłoby spełnić kryteria konieczne do objęcia funkcji kierowniczej w mniejszej, słabszej i uboższej AC niż większej, silniejszej i bogatszej ABW. Projektodawcy zrezygnowali zarazem z kryterium obecnego we wszystkich pozostałych służbach specjalnych, czyli konieczności cechowania się przez kandydata

„nieskazitelną postawą moralną, obywatelską i patriotyczną". To nie budzi zastrzeżeń, nawet więcej, sądzę, że należy rozważyć usunięcie tego uznaniowego kryterium z pozostałych ustaw. Rezygnacja z kryterium „posiada wyższe wykształcenie" (obowiązuje w CBA, SKW i SWW) jest dość zaskakująca, ale można interpretować to w ten sposób, że projektodawcy widzieliby na stanowisku szefa eksperta-praktyka, niezależnie od jego formalnego wykształcenia. Nie jest również przewidywane kryterium dotyczące bycia nieskazanym za przestępstwo popełnione umyślnie ścigane z oskarżenia publicznego lub za przestępstwo skarbowe. Trzeba zauważyć, że takie rozwiązanie przyjęto jedynie w ustawie o CBA. Opinia publiczna powinna mieć świadomość, że osoba skazana za kradzież z włamaniem nie może być w Polsce nauczycielem akademickim, ale może kierować kontrwywiadem. W odniesieniu do kandydatów na szefów wszystkich pięciu służb specjalnych stosowane jest również kryterium związane z piętnem uczestnictwa w komunistycznym aparacie represji. Na ich czele może stanąć jedynie osoba, która „nie pełniła służby zawodowej, nie pracowała i nie była współpracownikiem organów bezpieczeństwa państwa", wymienionych w katalogu ustawy o Instytucie Pamięci Narodowej. Nie może być to również „sędzia, który orzekając uchybił godności urzędu, sprzeniewierzając się niezawisłości sędziowskiej". W projekcie o AC takiego przepisu zabrakło. Zapewne po części dlatego, że lewica zdecydowanie odrzuca odpowiedzialność zbiorową w tym zakresie, czego wyrazem jest chociażby sprzeciw wobec przepisów tzw. drugiej ustawy dezubekizacyjnej (częściowo podzielam to stanowisko). Poza tym projektodawcy zakładają zapewne, że specjaliści od IT, którzy mieliby objąć to stanowisko, byli w okresie komunizmu dziećmi lub urodzili się już w III RP. Nie polemizując z tym założeniem, zwracam uwagę, że niewątpliwie zostanie dostrzeżone i oprotestowane.

Należy również nadmienić, że projektodawcy stawiają wyższe wymagania przed kandydatem do służby lub pracy w AC, niż przed kandydatem na jej szefa. Wymagana jest nie tylko „nieposzlakowana opinia", ale też brak skazania prawomocnym wyrokiem sądu za przestępstwo lub przestępstwo skarbowe oraz posiadanie wyższego wykształcenia (art. 28 ust. 1). Tak sztywnych przepisów w zakresie wykształcenia nie zawiera żadna z ustaw kompetencyjnych określających funkcjonowanie służb specjalnych. Wymóg posiadania wyższego wykształcenia jest zrozumiały (i praktykowany) w odniesieniu do oficerów, ale w odniesieniu do pracowników cywilnych z obszaru IT liczyć powinny się umiejętności praktyczne, a nie formalne wykształcenie. Przyjmując to rozwiązanie projektodawcy eliminują z postępowania kwalifikacyjnego wielu zdolnych hobbystów, którzy jeszcze nie ukończyli studiów lub nie mają zamiaru ich kończyć. Skoro w procesie naboru przewiduje się przeprowadzenie testu „wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru" (art. 28 ust. 3 pkt 2), to można zrezygnować z tego kryterium. W dalszej kolejności zakwalifikowane osoby można zachęcać do uzyskania wyższego wykształcenia w preferowanym przez służbę kierunku, oferując „urlopy sesyjne", premie czy dodatki służbowe.

Po dziewiąte, odwołanie Szefa AC z zajmowanego stanowiska miałoby odbywać się w trybie analogicznym z tym przyjętym w ustawach o ABW i AW oraz SKW i SWW. Wśród pięciu okoliczności (por. „po jedenaste") wymienia się skazanie „prawomocnym wyrokiem sądu za popełnione przestępstwo lub przestępstwo skarbowe" (art. 9 ust. 3). Okoliczność ta nie byłaby więc przeszkodą do objęcia stanowiska szefa AC, ale byłaby asumptem do jego utraty. Inaczej unormowane jest to w ustawie o CBA, w której niespełnianie któregokolwiek z warunków koniecznych do ubiegania się o stanowisko szefa jest zarazem okolicznością uzasadniająca jego odwołanie, co ma znaczenie

w odniesieniu do wspomnianej powyżej „nieskazitelności". Innymi słowy, szefowie ABW, AW, SKW i SWW muszą być „nieskazitelni" jedynie „na wejściu", a późniejszy brak owej „nieskazitelności" nie jest przesłanką do ich odwołania. Szef CBA musi być „nieskazitelny" przez cały czas, a jeśli nie jest, to może być w związku z tym odwołany (z tego przepisu skorzystał w 2009 r. premier Donald Tusk przerywając kadencję Mariusza Kamińskiego). Projektodawcy nie przewidują udziału tego uznaniowego kryterium ani na etapie powoływania, ani odwoływania szefa.

Po dziesiąte, projektodawcy wprowadzają ograniczenia dotyczące podziału obowiązków w kierownictwie AC (art. 11 ust. 2). Szef AC może przekazać swojemu zastępcy obowiązki dotyczące reprezentowania agencji w stosunkach prawnych z innymi podmiotami, zarządzania jej mieniem i wykonywania innych ustawowych zadań, ale nie może tego uczynić w odniesieniu do kierowania pracą AC i – co ciekawe – przedstawiania rocznej informacji o stanie cyberbezpieczeństwa państwa (kwestia, o której wspomniano w punkcie „po drugie" w części 2.5. niniejszego opracowania). To zbyt sztywne rozwiązanie, niepraktykowane w ustawach kompetencyjnych służb specjalnych. Wskazuje się w nich, że „szef (…) kieruje (…) bezpośrednio lub przez swoich zastępców". Wprowadzenie tego przepisu mogłoby doprowadzić do paraliżu służby w sytuacji tymczasowej niedyspozycji lub niedostępności szefa AC.

Po jedenaste, projektodawcy przewidują jednakowe wymagania wobec kandydatów na stanowiska szefa AC i zastępcy szefa AC, co jest praktykowane jedynie w CBA.

Po dwunaste, w projekcie zabrakło przepisu stanowiącego, że działalność szefa AC podlega kontroli Sejmu.

Po trzynaste, brakuje również przepisu wskazującego, że w celu realizacji zadań AC jej szef może podejmować współdziałanie z właściwymi organami i służbami innych państw. Podjęcie takiej współpracy powinno być możliwe jedynie po uzyskaniu zgody premiera (ewentualnie z udziałem innego organu w procedurze). To nie tylko rozwiązanie standardowe w odniesieniu do służb specjalnych, ale wymagane przez wewnętrzną logikę omawianego projektu. Instytucja, która miałaby pełnić funkcję organu ścigania w zakresie sprawców przestępstw z obszaru teleinformatyki, potrzebuje tego uprawnienia chociażby w kontekście jednego z najważniejszych wyzwań w obszarze cyberbezpieczeństwa – atrybucji.

Ponadto w art. 4 pkt 12 stwierdzono, że do zadań AC należy „wymiana informacji dotyczących zagrożeń cybernetycznych z właściwymi instytucjami podmiotami Unii Europejskiej, Organizacji Paktu Północnoatlantyckiego, Organizacji Narodów Zjednoczonych oraz Organizacji Bezpieczeństwa i Współpracy w Europie". Nie istnieje instytucja międzynarodowa o nazwie „Organizacja Paktu Północnoatlantyckiego". To nazwa potoczna, popularna z uwagi na militarne skojarzenia związane ze słowem „pakt". Angielski akronim brzmi przecież NATO („t" od „treaty"), a nie NAPO („p" od „pact"). Istnieje tylko jedna poprawna, formalna nazwa tej instytucji, używana zarówno w literaturze przedmiotu, jak i w polskim porządku normatywnym: Organizacja Traktatu Północnoatlantyckiego.

4. Budżet Agencji Cyberbezpieczeństwa

Projektodawcy wskazują, że działalność AC będzie finansowana z odrębnej części budżetu państwa (art. 5 ust. 1). Nie uściślono (wzorem ustawy o SKW i SWW), o którą część chodzi. Należy

zakładać, że byłaby to przede wszystkim część 754, czyli „Bezpieczeństwo publiczne i ochrona przeciwpożarowa".

Według propozycji projektodawców, koszt działania instytucji w latach 2022–2031 wyniósłby nie więcej niż 4,4 mld zł. Średnio byłoby to 440 mln zł rocznie, przy czym w latach 2022–2025, czyli w okresie organizowania instytucji, rósłby on stopniowo, od 117 mln zł w roku obecnym, do 765 mln zł w 2025 r., by następnie ustabilizować się na poziomie ponad 400 mln zł. AC byłaby więc najdroższą po ABW (ponad 600 mln zł) polską służbą specjalną, dystansując SKW (ponad 300 mln zł) oraz ABW, CBA i SWW (po ponad 200 mln zł).

Dla czytelnika, który uważnie śledzi zmiany prawa w zakresie aparatu bezpieczeństwa, kwoty te mogą brzmieć znajomo. Jest to bowiem dosłowne kopiuj-wklej z przygotowanego w MSWiA *projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości*, który 14 września 2021 r. został opublikowany przez Rządowe Centrum Legislacji. Dokładnie te kwoty znalazły się w wersji projektu, który trafił do Sejmu i został przegłosowany w grudniu.

Projektodawcy nie przeprowadzili więc żadnych samodzielnych kalkulacji dotyczących AC. Przejęli po prosty ministerialne wyliczenia dotyczące policyjnej instytucji mającej zatrudniać docelowo 1800 osób, której siedziba ma kosztować 450 mln zł. To tłumaczy, dlaczego postulatowi uruchomienia tak ogromnych środków nie towarzyszy informacja dotycząca tego, na co miałyby zostać spożytkowane. Można zrozumieć brak danych o planowanej szerokości szeregów instytucji (spośród służb specjalnych tylko CBA przedstawia dokładne dane w tym zakresie), ale jakikolwiek scenariusz wydatkowania powinien zostać zaprezentowany. To kolejny przykład dowodzący, że projektodawcy sami nie są pewni, czym miałaby być AC.

Symptomatyczne, że w ogóle nie wspomina się o planowanej siedzibie AC. Być może założono tymczasowe „zakwaterowanie" pracowników i funkcjonariuszy AC w kompleksie przy ul. Rakowieckiej, połączone z poszukiwaniem budynku do adaptacji lub gruntu pod jego budowę. Losy poszukiwania siedziby przez CBA (al. Ujazdowskie 5, al. Ujazdowskie 9, nieudana przeprowadzka na ul. Literacką 7) wskazują, że nie byłoby to łatwe i tanie rozwiązanie.

Gdyby AC rzeczywiście miała powstać, można by w tej sprawie rozważyć zastosowanie wariantu czeskiego. W 2011 r. w ramach Narodowego Centrum Bezpieczeństwa (*Národní bezpečnostní úřad*, NBU) z siedzibą w Pradze utworzono odpowiedzialną za cyberbezpieczeństwo komórkę – Narodowe Centrum Bezpieczeństwa Cybernetycznego (*Národní centrum kybernetické bezpečnosti*, NCKB). Nie powstała ona jednak w stolicy, tylko po drugiej stronie państwa – w Brnie. Siedzibę tę utrzymano po 2017 r., kiedy komórka została przekształcona w samodzielną instytucję – Krajowe Biuro Bezpieczeństwa Cybernetycznego i Informacji (*Národní úřad pro kybernetickou a informační bezpečnost*, NÚKIB). Jedną z przesłanek stojących za tą decyzją było istnienie w Brnie uczelni wyższych o profilu technicznym i firm z branży teleinformatycznej. Warunki tę spełnia wiele miast w Polsce, na czele z Krakowem, siedzibą Comarchu i Akademii Górniczo-Hutniczej im. Stanisława Staszica. Umiejscowienie AC poza Warszawą mogłoby stać się ważnym krokiem w niemal niestosowanej w Polsce delokalizacji administracji państwowej.

Ponadto proponowane jest ustalenie wielkości funduszu operacyjnego AC na poziomie maksymalnie 20% rocznego budżetu instytucji (art. 5 ust. 2). Rozumiem intencje autorów zmierzające do

wyegzekwowania transparentności i gospodarności w dysponowaniu funduszami służby, sądzę jednak, że jest to rozwiązanie zbyt sztywne, o możliwie patogennych konsekwencjach. Służba powinna dysponować pewną elastycznością w zakresie funduszu operacyjnego, dostosowując wydatkowanie do bieżącego zapotrzebowania. Co w sytuacji, gdy zabraknie środków na zakup lub aktualizację specjalistycznego sprzętu albo oprogramowania związanego z poważnym zagrożeniem nowego typu? Poza tym ustalając uznaniowo maksymalną wielkość funduszu operacyjnego sprzyja się prowadzeniu kreatywnej księgowości. Rachityczność lub zgoła fasadowość procedur w zakresie cywilnego nadzorowania i kontrolowania służb sprzyjałaby tego rodzaju nadużyciom.

5. Nazwa

Projektodawcy stanęli przed trudnym wyborem nazwy instytucji i związanego z nią akronimu. Przede wszystkim nazwa powinna możliwie wiernie odpowiadać funkcjom instytucji i jej systemowej pozycji. Należy wystrzegać się nazw zawiłych, żargonowych, generujących akronimy przywołujące niedobre skojarzenia, o wydźwięku humorystycznym czy trudnych w wymowie, a także zbliżonych brzmieniowo do akronimów instytucji już istniejącymi.

Projektodawcy proponują nazwanie nowej instytucji „agencją", zgodnie z polską i światową praktyką dotyczącą służb specjalnych. Przyjęto nazwę krótką i intuicyjną, co należy ocenić pozytywnie. Istnieją instytucje o analogicznej nazwie (np. singapurska *Cyber Security Agency*, CSA), co oznacza, że słusznie wpisano się w stosowane już rozwiązania.

Niewątpliwie komplikacją dla projektodawców było słowo „cyberbezpieczeństwo". Generuje ono „C" lub „CB" w akronimie, a więc w drugim wariancie mielibyśmy do czynienia z ACB, co doprowadziłoby do językowej kolizji z CBA. O literówkę byłoby nietrudno, słusznie zatem, że tej pułapki uniknięto. Powstały akronim nie jest moim zdaniem zbyt wygodny, „ace" brzmi, jakby czegoś w nazwie brakowało, ale to oczywiście kwestia subiektywna. Do nazwy można zgłosić jednak dwa poważniejsze zastrzeżenia.

Po pierwsze, jak dotąd pojęcie „agencja" w odniesieniu do polskich służb specjalnych używane było jedynie w odniesieniu do instytucji cywilnych, pełniących klasyczne funkcje: wywiadowczą (AW) i kontrwywiadowczą (ABW)[14]. Instytucja zajmująca się zwalczaniem korupcji w życiu publicznym i gospodarczym oraz działalności godzącej w interesy ekonomiczne państwa nazywana jest „biurem" (CBA), a wojskowy wywiad (SWW) i kontrwywiad (SKW) to „służby". W polskim systemie służb specjalnych – i w ogóle w systemie bezpieczeństwa wewnętrznego – więcej jest przypadkowości niż długofalowego namysłu, ale tym bardziej warto poszukiwać w nim wszelkich zrębów logiki i kierować konsekwencją. Skoro cywilne służby wywiadowcza i kontrwywiadowcza nazywane są „agencjami", a wojskowe – „służbami", natomiast CBA, specyficzna instytucja, która nie wpisuje się w klasyczne funkcje służb specjalnych, została nazwa „biurem", to może właśnie w tym kierunku należałoby pójść.

[14] Oczywiście obecnie realizacja zadań kontrwywiadowczych stanowi mniejszość działań podejmowanych przez ABW, ustępując miejsca problematyce zwalczania przestępczości gospodarczej i zorganizowanej. W istocie ABW jest policyjno-specjalną hybrydą, realizującą nie tylko funkcje typowe dla instytucji typu *domestic intelligence* i *counter-intelligence*, ale także zajmującą się ściganiem sprawców wybranych, poważnych przestępstw (*law enforcement*). Tego rodzaju hybrydą był też UOP, poprzednik ABW.

Po drugie, akronim w oczywisty sposób kojarzy się z ubezpieczeniem pojazdów mechanicznych. Projektodawcy powinni mieć świadomość, że w slangu służb ABW nazywane jest „Abwehrą". Agencja Cyberbezpieczeństwa byłaby najpewniej nazywana „Autocasco", „Allianzem" lub jakoś podobnie.

Można po prostu dopisać do nazwy „Narodowa" (NAC), wzorem Brytyjczyków, Włochów i Francuzów, ale domyślam, się, że projektodawcy nie będą zainteresowani takim pomysłem, sam zresztą jestem krytykiem nadużywania tego przymiotnika. Nie ma również takiej praktyki w zakresie instytucji bezpieczeństwa wewnętrznego i nie warto tworzyć precedensów. Określniki „Państwowa" lub „Polska" też nie rozwiązują problemu, powstałby bowiem akronim PAC, a lepiej uniknąć skojarzeń z „Pacanowem" i „pacanami" (na podobnej zasadzie UOP zatrudniał „jeuopów"). Lepszy byłby akronim Agencji Bezpieczeństwa Cybernetycznego (ABC), którą nazywano by zapewne „abecadłem".

Aby nie sięgać po nazwy bardziej rozbudowane i trudniejsze do zapamiętania, takie jak Agencja Bezpieczeństwa Technologii Informatycznych (ABTI), a także nie korzystać z pojęć już nieużywanych („urząd")[15], można pójść w zasugerowanym wcześniej kierunku i postulować utworzenie Centralnego Biura Cyberbezpieczeństwa (CBC). Niestety brzmi to dość podobnie do CBZC, które, w odróżnieniu od innej instytucji centralnej w strukturze Policji, Centralnego Biura Śledczego Policji (CBŚP), nie używa w swoim akronimie litery „P".

6. Uzasadnienie projektu

Towarzyszące projektowi uzasadnienie jest podręcznikowym przykładem tego, jak nie powinno wyglądać uzasadnienie projektu aktu normatywnego. Nie może ono sprowadzać się do „przepisania" proponowanych przepisów, tylko wyjaśniać ich sens i cel. Ponadto projektodawcy powinni wskazać, na czym polega różnica pomiędzy rozwiązaniami obowiązującymi a proponowanymi. Uzasadnienie omawianego projektu nie pełni żadnej z tych funkcji.

Podsumowanie

Zdarza się, że poselskie projekty ustaw nie są pełnoprawnymi propozycjami, tylko projektami projektów, wyrażającymi w najbardziej ogólnym zarysie podstawowe intencje pomysłodawców. Tak jest i w tym przypadku.

Poważne defekty widoczne są na każdym poziomie: sensowności generalnego założenia, jego kluczowych właściwości, rozwiązań szczegółowych, a także poprawności technicznej.

Pomysł utworzenia szóstej służby specjalnej zupełnie nie przekonuje. Już teraz Polska „bije rekordy" w tym zakresie, wyprzedzając Brytyjczyków czy Niemców. Powinniśmy raczej zmierzać w przeciwnym kierunku, zastanawiając się nad możliwością zespolenia niektórych służb lub części służb. Chodzi nie tyle o więcej centralizacji (mamy jej w nadmiarze), ale działania integracyjne. W zasadzie jedynym poważnym ruchem w tym kierunku wykonanym w okresie III RP było utworzenie Krajowej Administracji Skarbowej. Jej architektura nie jest wprawdzie czymś, co należy

[15] Nie chodzi wyłącznie o UOP. Warto przypomnieć, że instytucję, którą w 2006 r. nazwano Centralnym Biurem Antykorupcyjnym, kilka lat wcześniej planowano nazwać Centralnym Urzędem Antykorupcyjnym. Zob. *Poselski projekt ustawy o Centralnym Urzędzie Antykorupcyjnym*, druk nr 2025 z 19 IV 2000 r.

uznać za dobrą praktykę (w szczególności w zakresie Służby Celno-Skarbowej, czyli pozbawionej własnej struktury organizacyjnej formacji policyjnej w jej ramach), ale samą ideę należy ocenić pozytywnie. Pomysłów na dalsze kroki nie brakuje. Przykładowo Artur Gruszczak proponował utworzenie instytucji o roboczej nazwie Krajowe Biuro Śledcze, która zastąpiłaby CBŚP, Departament Postępowań Karnych ABW i biuro Generalnego Inspektora Informacji Finansowej. To ciekawy i ambitny kierunek, częściowo przywodzący na myśl rozwiązania, które rozważano jeszcze w okresie polskiej transformacji systemowej, a częściowo przypominający utworzoną w 2013 r. brytyjską Narodową Agencję ds. Przestępczości (National Crime Agency). Podobne postulaty integracyjne można formułować odnośnie do instytucji cyberbezpieczeństwa – miałyby one więcej sensu niż działanie w stronę pogłębienia rozproszenia.

Abstrahując od kwestii ewentualnego zespolenia, potrzebne jest wzmocnienie instytucji już istniejących, dofinansowanie ich oraz uszczelnienie procedur w zakresie nadzoru, kontroli, koordynowania i programowania.

Nie przekonuje również to, jak miałaby wyglądać AC. Jeśli faktycznie miałaby wykonywać czynności analityczno-informacyjne, operacyjno-rozpoznawcze i dochodzeniowo-śledcze (co jest niejasne) w odniesieniu do KITI i zagrożenia terrorystycznego, to powstałaby po prostu mniejsza kopia ABW. Ze wszech miar sensowniejszym pomysłem byłoby po prostu postulowanie rozbudowy ABW i CBZC. Tym, co w projekcie dziwi najbardziej, są propozycje ingerencji w ustawowe szczegóły przy jednoczesnym braku propozycji uregulowań o charakterze fundamentalnym.

W drugiej kolejności dziwią błędy w podstawowych sprawach. Nie jest dobrym znakiem, kiedy usterki merytoryczne można znaleźć nawet w treści proponowanych definicji (zob. art. 2 pkt 2, w którym pojawia się „przechowywanie lub przetwarzanie danych", zamiast samego „przetwarzanie danych" – „przetwarzanie" to pojęcie obejmujące kilkanaście czynności, w tym przechowywanie).

Na tym etapie nie sposób stwierdzić, czym, zdaniem pomysłodawców, miałaby być AC, po co miałaby powstać i jak miałaby się do innych elementów systemu. Polski system służb specjalnych obfituje w poważne dysfunkcje, ale przez ponad trzy dekady wypracowano w nim również szereg rozwiązań poprawnych, na czele ze standardami wskazanymi przez TK. W przygotowywaniu projektu ustawy o AC nie skorzystano jednak z tego dorobku.

Także w zakresie KSC propozycja projektodawców jest nieprzekonująca. Nie minęły jeszcze cztery lata obowiązywania ustawy o KSC, system dopiero niedawno „okrzepł". Z każdym rokiem jego podmioty mają coraz więcej pracy. Przykładowo w 2020 r. CSIRT GOV odnotował ponad 23 tys. incydentów teleinformatycznych, a w 2021 r. – ponad 26 tys. Należy zakładać, że obecny rok przyniesie kolejny rekord, być może spektakularny, do czego przyczynią się ciągłe zmagania z pandemią i konsekwencje rosyjskiej inwazji na Ukrainę. Te niestandardowe okoliczności tworzą zarazem dodatkowy powód, aby nie przeprowadzać w najbliższym czasie niepotrzebnych zmian w obszarze cyberbezpieczeństwa. Można na tego rodzaju uwagę odpowiedzieć kontrargumentem, że nigdy nie ma dobrego momentu na gruntowną reformę służb. To prawda, ale trudno wyobrazić sobie okoliczności mniej sprzyjające niż obecne.

Tym bardziej, że system działa całkiem sprawnie. Nic nie wskazuje na to, aby problematyka (słabości) koordynacji, którą projektodawcy stawiają na pierwszym miejscu, była faktycznie jego największą bolączką. Wydaje się, że na tym etapie największym wyzwaniem związanym z KSC nie są kwestie ustrojowe, tylko problemy kadrowe. Niedobór pracowników z obszaru IT jest problemem nie tylko dla polskiej administracji publicznej, ale także dla działających nad Wisłą podmiotów komercyjnych. Liczbę brakujących specjalistów z obszaru IT szacuje się czasem już nie w dziesiątkach, a setkach tysięcy. Postępująca cyfryzacja gospodarki i usług publicznych (*vide* rozwój ePUAP, Internetowe Konto Pacjenta z usługami e-recepta i e-skierowanie), zdynamizowana jeszcze przez pandemię, a także wzrost świadomości w zakresie cyberbezpieczeństwa będą zwiększały wagę tego deficytu. Utworzenie AC w niczym by w tym względzie nie pomogło, nawet przy założeniu, że pokaźny budżet służby umożliwiłby oferowanie kandydatom atrakcyjnych uposażeń. Już w ramach obecnych rozwiązań systemowych można zmierzać w kierunku uczynienia pracy lub służby w instytucjach odpowiedzialnych za cyberbezpieczeństwo atrakcyjną na równi z zatrudnieniem w sektorze prywatnym. Taką zmianę ostatnio przeforsował rząd i można dalej zmierzać w tę stronę. Potrzebna jest promocja kariery związanej z cyberbezpieczeństwem i rozbudowa oferty programowej studiów w tym zakresie. Tak więc jest to sprawa, która powinna być rozważana nie tylko w kontekście służb specjalnych, ale także (a może przede wszystkim) działów administracji rządowej: praca oraz szkolnictwo wyższe i nauka.

Innym pomysłem do rozważenia jest zwiększenie nakładów i zdynamizowanie działań obliczonych na rozwój potencjału naukowo-technicznego Polski w zakresie cyberbezpieczeństwa. Wiele państw tworzy tego rodzaju wyspecjalizowane komórki, wzorując się na amerykańskich ARPA-ch, czyli sieci agencji zapoczątkowanej przez słyną Agencję Zaawansowanych Projektów Badawczych w Obszarze Obronności (*Defense Advanced Research Projects Agency*, DARPA). Instytucja, której można by powierzyć w Polsce tę funkcję, już istnieje: Narodowe Centrum Badań i Rozwoju (NCBR). Budżet, którym dysponuje, na papierze wygląda okazale: w 2020 r. przekazało wnioskodawcom ponad 5 mld zł. Ale programy krajowe pochłonęły tylko niecałe 790 mln zł, z czego niecałe 234 mln zł wydano na projekty na rzecz obronności i bezpieczeństwa. Warto zauważyć, że jednym z programów krajowych NCBR jest CyberSecIdent, nakierowanym na podniesienie bezpieczeństwa polskiej cyberprzestrzeni. W jego ramach w 2020 r. przekazano beneficjentom ponad 31 mln zł, czyli mniej więcej tyle, ile wynosi budżet Piasta Gliwice w obecnym sezonie Ekstraklasy. Zważywszy na fakt, że projektodawcy proponowali, aby przez najbliższą dekadę z budżetu państwa płynęło do AC średnio 440 mln zł rocznie, można zastanawiać się, czy bardziej perspektywicznym rozwiązaniem nie byłoby na przykład dziesięciokrotne rozbudowanie programu CyberSecIdent.

Ważne zmiany do systemu wprowadzi transpozycja kolejnej dyrektywy UE, Europejskiego Kodeksu Łączności Elektronicznej (2018/1972). Ustawa Prawo komunikacji elektronicznej, która ma zastąpić ustawę Prawo telekomunikacyjne z 2004 r., powinna była zostać przyjęta do końca 2020 r., ale tak się nie stało. Obecny plan rządu zakłada zakończenie prac w 2022 r. i wejście w życie nowej ustawy 1 stycznia 2023 r. W roku bieżącym mają również zakończyć się prace nad nowelizacją ustawy o KSC. Także te okoliczności trzeba brać pod uwagę w kontekście tworzenia AC.

Projektodawcy krytykują więc KSC od strony bardzo rzadko spotykanej w refleksji ekspertów i naukowców. Pomijają natomiast te jego aspekty, które faktycznie spotykają się z zastrzeżeniami, np. słabość ścigania sprawców incydentów komputerowych. W systemie nie może chodzić wyłącznie

o to, aby wykryć, zgłosić i zanalizować incydent, a następnie wyciągnąć z niego wnioski, ale także o atrybucję i pociągnięcie do odpowiedzialności sprawcy. Zdecydowana większość incydentów wiąże się przecież z naruszeniem prawa. Tym samym można zastanawiać się nad wzmocnieniem roli organów ścigania w KSC. Tego wątku projektodawcy jednak nie podejmują.

Autorzy projektu mają rację uwypuklając rolę profilaktyki i informowania. Dobry kontrwywiad zaczyna się w domu, chociażby od prostych praktyk związanych z podejściem do danych osobowych. Nie inaczej jest z cyberbezpieczeństwem. Ogromna część incydentów komputerowych ma prosty w sensie technicznym charakter. Coraz popularniejsze ataki phishingowe nie bazują na zaawansowanych rozwiązaniach informatycznych, tylko na prostej socjotechnice i braku wiedzy użytkowników. Do prowadzenia profilaktyki i promocji dobrych praktyk nie jest jednak potrzebna nowa służba specjalna. Do szkolenia specjalistów „wewnętrznych", czyli będących częścią KSC, można wykorzystać struktury już istniejące, sukcesywnie rozbudowując je kadrowo i ofertowo. Także promowanie i wdrażanie dobrych praktyk w szeregowych strukturach administracji publicznej nie wymaga angażowania służby specjalnej. Nie wspominając o kształtowaniu odpowiedzialnych postaw społeczeństwa, w czym kluczową rolę do odegrania mają nie instytucje bezpieczeństwa, tylko oświata i szkolnictwo wyższe.

Bardzo ważną funkcję w systemie pełnią organy samorządu terytorialnego, przetwarzające wielką liczbę danych i mające znaczny wpływ na funkcjonowanie wielu usług publicznych. Potrzebne jest ich wspieranie merytoryczne i finansowe, a także szeroko zakrojone mechanizmy egzekwowania stosowania się do standardów cyberbezpieczeństwa. Duże znaczenie dla usuwania słabych punktów systemu miałby rozwój inicjatyw takich jak Regionalne Centrum Bezpieczeństwa Cybernetycznego czy stworzenie rozwiązań sprzyjających powstawaniu sektorowych zespołów cyberbezpieczeństwa. Te sprawy w projekcie w ogóle się nie pojawiają.

Zasadnym postulatem o charakterze generalnym jest wymuszenie na służbach większej transparentności – zwłaszcza na tych, które prowadzą czynności dochodzeniowo-śledcze. Pożądaną zmianą byłoby na przykład odejście od centralizacji prowadzenia przez nie komunikacji społecznej (czyli przywrócenie odrębnych rzeczników) czy rozbudowa obowiązku sprawozdawczości i informowania. Są to propozycje, których realizacja nie wymaga wprawdzie zmiany materii ustawowej, ale warto zabiegać, aby przyjęła właśnie taką formę. Do jakiejkolwiek aktywności informacyjnej ukierunkowanej na opinię publiczną należałoby zmusić służby wywiadowcze, zwłaszcza cywilne. Tocząca się tuż za naszą granicą wojna nie jest najlepszym momentem, aby zajmować się komiksem o Enigmie (*vide* twitterowe konto AW). Oba nasze wywiady milczą. Ta hipertajność nie robi na nikim wrażenia, generuje raczej domysły, że są bezczynne (co z pewnością nie jest prawdą) lub że nie mają nic ciekawego do powiedzenia. Nie chodzi nawet o to, aby przyjąć model Brytyjczyków, którzy publikują regularny biuletyn *intelligence update* poświęcony rosyjskiej inwazji na Ukrainę, ale o chociażby minimalną medialną obecność. Tego oczywiście zapisać w prawie się nie da, potrzebny jest nacisk opinii publicznej. A i same służby powinny rozumieć, że tego rodzaju aktywność jest również w ich długofalowym interesie.

Autorzy projektu słusznie podkreślają znaczenie koordynacji. Nie zauważają jednak, że jego uchwalenie doprowadziłoby do dalszego zagmatwania systemu. W opublikowanej kilka miesięcy temu analizie napisałem: „Przypadkowości polityki bezpieczeństwa wewnętrznego, czyli jego ce-

sze wiodącej, towarzyszą cztery zazębiające się zjawiska: inercja, bieda, fragmentaryzacja i centralizacja". Realizacja omawianej propozycji nie tylko nie odwróciłaby tego negatywnego trendu, ale wręcz mogłaby przyczynić się do jego wzmocnienia.