UCHWAŁA nr 1
RADY do SPRAW CYFRYZACJI

z dnia 31 stycznia 2022 roku
w sprawie powołania Centralnego Biura Zwalczania Cyberprzestępczości.

Na podstawie art. 17 ust. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 2070) oraz § 5 Regulaminu Rady do Spraw Cyfryzacji stanowiącego załącznik do Zarządzenia nr 17 Ministra Cyfryzacji z dnia 24 czerwca 2020 r. w sprawie ustanowienia regulaminu Rady do Spraw Cyfryzacji (Dz. Urz. z 2020 r. poz. 19), uchwala się, co następuje:

W związku z obserwowanym w Polsce stałym wzrostem ilości incydentów klasyfikowanych przez zespoły CSIRT NASK i CSIRT ABW, wzrostem liczby postępowań prowadzonych w sprawach z zakresu cyberprzestępczości oraz zmianą sposobu działania sprawców popełniających czyny, które często pomijane są w analizach dotyczących zjawiska cyberprzestępczości (dla przykładu 42 % oszustw klasyfikowanych na postawie art. 286 § 1-3 k.k. opisanych jest w policyjnych bazach danych jako „internetowe", ich ilość w okresie od 2016 do 2020 roku wzrosła o 30 %), za krok w dobrym kierunku uznać należy utworzenie Centralnego Biura Zwalczania Cyberprzestępczości (CBZC). Zgodnie z ustawą z dnia 17.12.2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz.U. poz. 2447), Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) ma być jednostką organizacyjną Policji - służbą zwalczania cyberprzestępczości odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie: rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, wykrywania i ścigania ich sprawców oraz zapobiegania tym przestępstwom. Ponadto CBZC wspierać ma w niezbędnym zakresie jednostki organizacyjne Policji w rozpoznawaniu, zapobieganiu i zwalczaniu tych przestępstw oraz wykrywaniu i ściganiu ich sprawców.

Zakres zadań nowej służby nie został określony poprzez wskazanie kwalifikacji prawnych, na podstawie których zainicjowane zostało postępowanie, lecz niezwykle ogólnie poprzez wskazanie, że chodzi o przestępstwa popełnione przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej. Z jednej strony zapewnia to elastyczność, z drugiej jednak należy zwrócić uwagę, że przy pomocy wskazanych systemów i sieci popełniane są różne kategorie czynów (np. kierowanie gróźb karalnych, zniesławienie czy stalking za pośrednictwem środków komunikacji elektronicznej). Niezwykle ogólne określenie zakresu zadań nowej służby może prowadzić do tego, że przy ograniczonym zasobie kadrowym, nie będzie mogła ona skupić się na postępowaniach najpoważniejszych i najbardziej skomplikowanych (wobec zorganizowanych grup przestępczych, o transgranicznym charakterze, gdzie występuje znaczna szkoda). Jest to

szczególnie ważne w czasie kiedy cybernarzędzia można kupić, a cyberprzestępczość staje się usługą i modelem biznesowym. Największym zagrożeniem jest w tym przypadku „Ransomware as a Service", trend, który doprowadził do wykładniczego wzrostu liczby ataków ransomware na całym świecie w samym III kwartale 2020 r. o 40%, do 199,7 mln przypadków.

Dodatkowo wskazano, że do zakresu zadań CBZC należy również wspieranie w niezbędnym zakresie pozostałych jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, a także wykrywania i ścigania sprawców tych przestępstw. Rodzi to obawę, że inne jednostki zlecały będą CBZC wykonywanie czynności, które mogą przeprowadzić samodzielnie (oględziny monitoringu, OSINT) lub powołując do ich wykonania biegłego z zakresu informatyki śledczej (np. ekstrakcja danych z telefonów komórkowych). Dlatego też należy wspierać działania mające na celu podniesienie kompetencji wszystkich funkcjonariuszy Policji, poprzez system stałych szkoleń z zakresu cyberprzestępczości – w tym z zakresu zabezpieczania danych i informatycznych nośników danych. Z drugiej zaś strony, w zawiązku brakiem jednoznacznie określonej właściwości rzeczowej CBZC wiele postępowań z zakresu cyberprzestępczości będzie prowadzonych przez inne jednostki organizacyjne Policji, co może skutkować brakiem realizacji celów postępowania, z uwagi na brak wykwalifikowanych funkcjonariuszy zajmujących się cyberprzestępczością w innych jednostkach.

Dla sprawnej realizacji zadań związanych ze zwalczaniem cyberprzestępczości niezbędne jest zapewnienie zasobu kadrowego. Zgodnie ze zmienianym art. 25 ustawy o Policji kandydaci do służby w CBZC będą musieli spełniać ogólne warunki określone w art. 25 ust. 1 ustawy o Policji, według którego służbę w Policji może pełnić obywatel polski o nieposzlakowanej opinii, który nie był skazany prawomocnym wyrokiem sądu za przestępstwo lub przestępstwo skarbowe, korzystający z pełni praw publicznych, posiadający co najmniej wykształcenie średnie lub średnie branżowe oraz zdolność fizyczną i psychiczną do służby w formacjach uzbrojonych, podległych szczególnej dyscyplinie służbowej, której gotów jest się podporządkować, a także dający rękojmię zachowania tajemnicy stosownie do wymogów określonych w przepisach o ochronie informacji niejawnych. Przyjęcie do CBZC ma następować po przeprowadzeniu postępowania kwalifikacyjnego mającego na celu ustalenie, czy kandydat spełnia warunki przyjęcia do służby w Policji oraz określenie jego predyspozycji do pełnienia tej służby. W postępowaniu kwalifikacyjnym do CBZC pomięte zostały niektóre z etapów. W szczególności brak jest wymagania dotyczącego testów sprawności fizycznej, zaś w art. 25 ust. 12 lit. d pozostawiono jedynie etap „ustalenia zdolności fizycznej i psychicznej do służby w Policji". Należy pamiętać, że CBZC będzie formacją prowadzącą pracę operacyjną oraz postępowania przygotowawcze, z czym wiąże się konieczność brania udziału w zatrzymaniach, przeszukaniach i tym podobnych czynnościach o dynamicznym przebiegu. Dlatego też celowe jest pozostawienie podstawowych etapów postępowania kwalifikacyjnego, z zapewnieniem Komendantowi

CBZC możliwości ewentualnego ograniczenia wymagań szczególnych w uzasadnionych przypadkach - np. w zakresie postępowania kwalifikacyjnego dotyczącego specjalistów z zakresu informatyki śledczej (możliwość ta jest wskazana w art. 25 ust. 5 ustawy o Policji).

Dodatkowo w stosunku do kandydata ubiegającego się o przyjęcie do służby zwalczania cyberprzestępczości na stanowisko związane z bezpośrednim rozpoznawaniem, zapobieganiem i zwalczaniem przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, a także wykrywaniem i ściganiem sprawców tych przestępstw, postępowanie kwalifikacyjne składa się z etapu sprawdzenia wiedzy i umiejętności z zakresu informatyki, funkcjonowania systemów informatycznych, systemów teleinformatycznych, sieci teleinformatycznych oraz znajomości języka obcego z tego obszaru.

Jednocześnie z uwagi na to, że funkcjonariusze CBZC wykonywali będą zróżnicowane zadania związane zarówno z różnymi formami pracy operacyjnej, prowadzeniem postępowań przygotowawczych czy informatyką śledczą, należy rozważyć, czy jednolity wymóg związany ze sprawdzeniem wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru, nie ograniczy możliwości przyjęcia do służby doświadczonych dochodzeniowców lub funkcjonariuszy operacyjnych, którzy dotychczas pracowali w wydziałach przestępczości gospodarczej. Wymagania dotyczące wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii powinny być zróżnicowane w zależności od komórki organizacyjnej oraz zadań, które poszczególne grupy funkcjonariuszy będą wykonywać. Również znajomość języka obcego z zakresu informatyki i nowoczesnych technologii teleinformatycznych nie będzie kluczowa na niektórych stanowiskach służbowych. Inny jest zakres wiedzy i umiejętności, który powinien być wymagany od funkcjonariusza, który będzie prowadził postępowanie przygotowawcze (tzw. dochodzeniowiec), inne wobec funkcjonariuszy operacyjnych, jeszcze inne wobec osób zajmujących się informatyką śledczą, współpracą międzynarodową czy analizą kryminalną, w sprawach z zakresu cyberprzestępczości. Wymagany poziom znajomości języka oraz specjalistyczne słownictwo z zakresu informatyki i nowoczesnych technologii, powinny być dostosowane do stanowisk służbowych czy zadań funkcjonariuszy w poszczególnych komórkach organizacyjnych. Zakres tematyczny sprawdzenia wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru, ma zostać określony w drodze rozporządzenia przez ministra właściwego do spraw wewnętrznych. „Zakres tematyczny z zakresu wiedzy i umiejętności CBZC" wskazany w projekcie rozporządzenia w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji określony jest niezwykle chaotycznie i nie odnosi się do zróżnicowanych zadań, jakie będą realizowane przez służbę zwalczania cyberprzestępczości.

Trzon kadrowy CBZC stanowić mają funkcjonariusze Biura do Walki z Cyberprzestępczością Komendy Głównej Policji, wydziałów do walki z cyberprzestępczością komend wojewódzkich (Stołecznej) Policji. W tym miejscu należy zwrócić uwagę, że aktualnie istniejący pion do

walki z cyberprzestępczością dysponuje nielicznym zasobem kadrowym i obejmuje w całej Polsce ok. 330 osób, z czego około 50 osób w Biurze dw. z Cyberprzestępczością KGP. Zgodnie z zapowiedziami docelowo CBZC ma liczyć 1 800 funkcjonariuszy. Konieczne będzie zatem pozyskanie około 1 500 funkcjonariuszy posiadających wiedzę i umiejętności z zakresu informatyki i nowoczesnych technologii teleinformatycznych oraz znajomości języka obcego z tego obszaru. Niewątpliwie w procesie powstawania CBZC kluczowe będzie pozyskanie doświadczonych dochodzeniowców (w szczególności z pionów PG), a także specjalistów zajmujących się informatyką śledczą, programistów, informatyków zajmujących się cyberbezpieczeństwem. Może to rodzić problemy z naborem lub powodować deficyty kadrowe związane z odpływem funkcjonariuszy z innych jednostek. Kluczowe jest zatem zapewnienie stałego naboru do Policji oraz zróżnicowanych form kształcenia funkcjonariuszy, którzy chcieliby specjalizować się w zwalczaniu cyberprzestępczości.

Celu tego aktualnie nie realizują w wystarczającym stopniu szkoły policyjne, a specjalistyczne kształcenie z zakresu zwalczania cyberprzestępczości prowadzone przez wiele lat w Wyższej Szkole Policji w Szczytnie zostało znacząco ograniczone, również poprzez likwidację kierunku nauczania w obszarze cyberbezpieczeństwa i likwidacji zakładu zajmującego się badaniami i edukacją w obszarze zwalczania cyberprzestępczości, a wykwalifikowani pracownicy naukowo – dydaktyczni z tego zakresu odeszli. Problemy natury kadrowej wydaje się potwierdzać fakt, że sygnalizowane plany rekrutacji, mówiące o pozyskaniu w pierwszym roku funkcjonowania ustawy około 300 specjalistów, przy jednoczesnej likwidacji obecnych struktur, w praktyce nie oznaczają żadnej jakościowej i ilościowej zmiany w odniesieniu do wzmacniania kadr zajmujących się tym zjawiskiem.

Równie ważne jest to, że strategia wzmocnienia ośrodka zwalczania cyberprzestępczości, głównie w oparciu o czynnik kadrowy, bez strukturalnego zapewnienia ustawicznego pozyskiwania nowych kadr w oparciu o działania edukacyjne, z dużym prawdopodobieństwem może prowadzić do zjawiska tzw. „kanibalizacji kadrowej" w obszarze całości systemu cyberbezpieczeństwa sektora publicznego. Byłoby to zjawisko bardzo niebezpieczne dla funkcjonowania tego systemu w odniesieniu do bezpieczeństwa Państwa.

Co więcej, wyodrębnienie Centralnego Biura Zwalczania Cyberprzestępczości nie podniesie poziomu wykrywczości, jeśli nie zostaną zmienione przepisy dotyczące możliwości pozyskiwania i gromadzenia danych niezbędnych do prowadzenia ustaleń w sprawach z zakresu cyberprzestępczości, zmiany w kodeksie karnym i kodeksie postępowania karnego.

Jako krok w dobrym kierunku uznać należy rozszerzenie katalogu czynów wskazanych w art. 19 ust. 1 pkt 2 ustawy o Policji, co ułatwi prowadzenie czynności operacyjno-rozpoznawczych w sprawach z zakresu cyberprzestępczości (aktualnie alternatywą pozostaje w tych sprawach oparcie się o art. 19 ust. 1 pkt 8 ustawy o Policji, odnoszący się do przestępstw ściganych na mocy umów międzynarodowych ratyfikowanych za uprzednią zgodą wyrażoną w ustawie, określonych w polskiej ustawie karnej oraz konwencję Rady Europy o cyberprzestępczości, sporządzoną w Budapeszcie dnia

23 listopada 2001 r. (Dz.U. z 2015 r. poz. 728)). Czyn z art. 267 § 1 k.k. zagrożony jest jednak karą do 2 lat pozbawienia wolności i ścigany jest na wniosek pokrzywdzonego. Projekt ustawy podnosi zagrożenie karne wyłącznie dla sprawców tzw. „kaskadowych alarmów bombowych", nie obejmując innych niezbędnych zmian w k.k. W zakresie zmian w art. 19 a ust. 1 i 2 ustawy o Policji, do rozważenia pozostaje dodanie możliwości nabycia, zbycia lub przejęcia nie tylko „przedmiotów", ale również „danych". Zarówno w karnomaterialnym jak i karnoprocesowym znaczeniu pojęcie „przedmiotu" czy „rzeczy" jest bowiem rozróżniane od pojęcia „danych". Zmiana ta jest celowa w kontekście zwiększenia skuteczności ścigania cyberprzestępczości i umożliwi np. nabycie pochodzącego z przestępstwa zbioru danych (który oderwany jest od przedmiotu w postaci informatycznego nośnika danych), w celu ustalenia sprawców przestępstwa.

W opiniowanej ustawie nie ma budzącego największe kontrowersje art. 19c (z wersji projektu z dnia 27 lipca 2021 roku), tym samym Centralne Biuro Zwalczania Cyberprzestępczości nie zyska dodatkowych uprawnień, zwiększających możliwości wykrycia sprawców cyberprzestępstw używających narzędzi anonimizujących.

Projekt nie odnosi się do rozwiązania problemów, które są realnym utrudnieniem prowadzenia spraw z zakresu cyberprzestępczości tj.:

- Niskiej wiarygodności danych abonentów przedpłaconych usług telekomunikacyjnych (z uwagi na powszechny obrót kartami SIM zarejestrowanymi na dane innych osób).
- Niskiej wiarygodności danych dotyczących rejestracji nazw domenowych w domenie .pl (z uwagi na brak weryfikacji tożsamości abonentów) oraz ograniczonym dostępem do danych przez bazę WHOIS, w zakresie abonentów będących osobami fizycznymi.
- Braku przepisów regulujących gromadzenie logów, ich strukturę oraz ustalenia okresu ich przechowywania (brak jest retencji danych „internetowych" np. w zakresie logowania do poczty elektronicznej).
- Stosowania NAT w sieciach (przy jednoczesnym niegromadzeniu przez większość podmiotów - w tym banki - numerów portów, co uniemożliwia ustalenia sprawców na podstawie adresów IP).
- Spoofingu numerów telefonów.
- Trybu zwolnienia z tajemnicy bankowej (aktualnie jeden muł finansowy („słup") jest w stanie założyć od kilku do kilkunastu rachunków w kilku – kilkunastu bankach. Brak wymiany danych pomiędzy bankami powiązany z ochroną tajemnicy bankowej i czasochłonnym procesem pozyskiwania danych na potrzeby postępowań karnych sprawia, że niezwykle trudne jest ustalenie takich rachunków, zablokowanie środków finansowych na nich zgromadzonych oraz ustalenie sprawców na podstawie analizy *follow the money*).

- Zmian znamion przestępstwa kradzieży tożsamości (art. 190 a § 2 k.k.).
- Zmian w k.p.k. w zakresie przeszukania zdalnego, przeszukania rozszerzonego, oględzin (danych) czy eksperymentu procesowego.

Ponadto za zmianami w strukturach policji podążać powinny również zmiany w strukturach prokuratury – polegające w szczególności na tworzeniu działów do spraw cyberprzestępczości w prokuraturach okręgowych i regionalnych oraz zwiększeniu koordynacji postępowań z tego zakresu.

Rada popiera kierunek polegający na wzmocnieniu sił policyjnych dedykowanych do walki z cyberprzestępczością, jednak dostrzega, że samo utworzenie nowej służby w ramach Policji jest niewystarczające. Działaniom tym powinny towarzyszyć również zmiany związane ze zwiększeniem koordynacji działań podmiotów tworzących krajowy system cyberbezpieczeństwa, zmiany kodeksu karnego, kodeksu postępowania karnego oraz ustaw szczególnych odnoszących się do gromadzenia i przekazywania danych niezbędnych do wykrycia i analizy incydentów.

Jako alternatywne lub dodatkowe rozwiązanie dla CBZC warto rozważyć jego funkcjonowanie jako podmiotu, który pełni funkcję pomocniczą w stosunku do innych komórek organów ścigania, wspierając je w działaniach związanych z koniecznością analizy tych elementów działalności przestępczej, które są prowadzone z wykorzystaniem technik teleinformatycznych.

W tym modelu prowadzenie śledztw realizowane byłoby przez wydziały policji wg podstawowej kwalifikacji czynu przestępczego. Natomiast Biuro włączone byłoby w te działania, które wymagają kompetencji i narzędzi koniecznych do skutecznej realizacji sprawy. Do działań takich można zaliczyć zaawansowane analizy teleinformatyczne (np: analiza złośliwego oprogramowania, informatyka śledcza), współdziałanie z krajowymi podmiotami zewnętrznymi (np: operatorami telekomunikacyjnymi, podmiotami krajowego systemu cyberbezpieczeństwa, np: CSIRT-ami), czy współdziałanie na płaszczyźnie międzynarodowej (np: z innymi organami ścigania, w szczególności powołanymi do zwalczania cyberprzestępczości).

Tego typu podejście, o charakterze horyzontalnym, a nie wertykalnym, ograniczyłoby ryzyko niewystarczającej współpracy pomiędzy funkcjonariuszami działającymi w obszarze cyberprzestrzeni i tymi, którzy prowadzą tradycyjne działania operacyjne. Jest to o tyle ważne, że skuteczne ściganie zdecydowanej większości przestępstw, bez zapewnienia obydwu elementów (cyber i tradycyjnego) jest w praktyce niemożliwe. Ustawa z dnia 17 grudnia 2021 roku wprawdzie wskazuje na zadania związane ze wspieraniem innych jednostek organizacyjnych Policji, jednak pozostaje bardzo prawdopodobne, że wyodrębnienie pionu zwalczania cyberprzestępczości do CBZC, finalnie przyczyni się do ograniczenia wsparcia, dotychczas zapewnianego przez Wydziały dw. z Cyberprzestępczością w Komendach Wojewódzkich Policji.

Protokół z głosowania

Decyzją Przewodniczącego Rady głosowanie zostało przeprowadzone w trybie obiegowym. Projekt uchwały nr 1 został przesłany członkom Rady 26 stycznia 2022 r. z terminem głosowania do 31 stycznia 2022 r. W głosowaniu wzięło udział 16 członków Rady, z czego oddano:

- 16 głosów „za" przyjęciem uchwały,
- 0 głosów „przeciw" oraz
- 0 głosów „wstrzymuję się".

Uchwała nr 1 Rady do Spraw Cyfryzacji została przyjęta 31 stycznia 2022 roku w głosowaniu jawnym w trybie obiegowym zwykłą większością głosów.

Szczegóły dotyczące głosowania przedstawia poniższa tabela.

Lp.	Imię	Nazwisko	Głos
1.	Izabela	Albrycht	za
2.	Katarzyna	Chałubińska-Jentkiewicz	za
3.	Konrad	Ciesiołkiewicz	za
4.	Andrzej	Dulka	za
5.	Agnieszka	Gryszczyńska	za
6.	Michał	Kanownik	za
7.	Janusz	Kosiński	za
8.	Karol	Krawczyk	za
9.	Anna Beata	Kwiatkowska	za
10.	Mirosław	Maj	za
11.	Dariusz	Milka	za
12.	Aleksandra	Musielak	za
13.	Bolesław	Piasecki	za
14.	Robert	Trętowski	za
15.	Mateusz	Tykierko	za
16.	Marcin	Zarzecki	za

Przewodniczący Rady
Józef Orzeł
/-podpisano elektronicznie/