PROTOKÓŁ z XIX posiedzenia Rady do Spraw Cyfryzacji, które odbyło się 15 października 2021 roku, o godzinie 13:00 w formie wideokonferencji.

Projekt ustawy o powołaniu Centralnego Biura Zwalczania Cyberprzestępczości – Pani Agnieszka Gryszczyńska, Pan Mirosław Maj; Pan insp. Sławomir Szumilas, Zastępca Dyrektora Biura do walki z cyberprzestępczością (Biuro) Komendy Głównej Policji oraz Pan Mariusz Cichomski, Dyrektor Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji.

Pani Agnieszka Gryszczyńska przypomniała, że posiedzenie Rady poświęcone jest analizie projektu ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości. W związku z tym przedstawiła prezentację wprowadzającą w tematykę posiedzenia. Zwróciła uwagę, że należy rozgraniczyć dwa problemy: incydentów i ich obsługi od problemu cyberprzestępczości i jej zwalczania. Zdecydowana część incydentów, które można zaobserwować, stanowią czyn zabroniony, ale nie wszystkie. Przestępstwo jest wąsko zdefiniowane w kodeksie karnym (art. 1 k.k) jako czyn, zabroniony pod groźbą kary przez ustawę obowiązującą w czasie jego popełnienia, bezprawny, zawiniony, społecznie szkodliwy w stopniu wyższym niż znikomy. Pojęcie incydentu jest pojęciem szerszym.

W raportach zespołów CSIRT GOV za 2020 r. oraz CSIRT NASK został zaobserwowany dramatyczny wzrost ilości zgłoszeń oraz incydentów. Wzrost ilości zgłoszeń jest pochodną ustawy o Krajowym Systemie Cyberbezpieczeństwa i popularyzacji procedury zgłaszania incydentów. Incydenty zaobserwowane przez Zespół CSIRT NASK są to oszustwa komputerowe w tym phishing, czyli ataki sprawców ukierunkowanych na monetyzację takiego ataku.

W 2020 r. w raporcie CSIRT NASK było ponad 10 tys. przeanalizowanych incydentów. W I połowie 2021 przekroczone zostało 10 tys., co świadczy że tematyka jest niezwykle aktualna i ważna na tyle, że trzeba zadać pytanie, czy nasz system ochrony przed incydentami oraz zwalczania cyberprzestępczości działa poprawnie. Raporty ukazują, że większość incydentów są to przestępstwa. W policyjnych statystykach zaobserwowano dynamiczny wzrost w kategorii zarówno przestępstwa z art. 267 § 1 k.k. nazywanego hackingiem oraz 287 § 1 k.k., czyli oszustwa komputerowego, jednak postepowań wszczętych na tych podstawach nie jest dużo.

Nie tylko z tych kwalifikacji wszczynane są postępowania. 42 % wszystkich oszustw kwalifikowanych na podstawie art. 286 § 1-3 k.k. jest zaznaczone w policyjnych bazach danych jako oszustwa internetowe, co stanowi istotny problem. Aktualnie z cyberprzestępczością walczy ABW jednak w wąskiej właściwości. Zdecydowana większość postepowań jest prowadzonych przez policję, gdzie znajduje się Biuro.

Poza Biurem istnieją wydziały do walki z cyberprzestępczością w Komendach Wojewódzkich Policji. Istniejący pion zwalczania cyberprzestępczości prowadzi postępowania duże i poważne. Aktualnie, bardzo poważne postępowania, realizowane z sukcesem prowadzone są również przez CBŚP.

W odniesieniu do wersji pierwotnej obecny projekt wprowadza daleko idące zmiany. Zmiana ustawy o Policji miała wyodrębnić nowy rodzaj służby w Policji – zwalczania cyberprzestępczości. Projekt ten nie obejmuje wszystkich problemów, ponieważ nie odnosi się do cyberbezpieczeństwa. W uwagach zgłaszanych m.in. przez Prokuraturę Krajową dotyczących rozbudowania przepisów, które stwarzają dodatkowe uprawnienia oraz możliwości ustalania sprawców i ich ścigania, otrzymano odpowiedź, że projekt odnosi się tylko do kwestii organizacyjnych i wyodrębnienia nowej służby, nie ma zaś szerokiego zakresu zmiany przepisów odnoszących się np. do gromadzenia danych, poszerzenia dolnej granicy zagrożenia karnego dla poszczególnych typów przestępstw. W wersji aktualnej tego projektu jest wprowadzona zmiana jednego przepisu kodeksu karnego tj. kaskadowe alarmy bombowe - górne i dolne zagrożenie karne ma zostać podniesione.

Dalsza dyskusja w ramach posiedzenia Rady miała na celu odpowiedzieć na pytanie, czy stworzenie nowej formacji rozwiąże problem, ewentualnie przyczyni się do podniesienia skuteczności zwalczania cyberprzestępczości i stworzy możliwości, których oczekują funkcjonariusze tego pionu.

Głos zabrał Pan Dyrektor Sławomir Szumilas wskazując problemy z jakimi obecnie borykają się wydziały do walki z cyberprzestępczością. Pan Dyrektor wskazał, że duża część problemów została wymieniona przez Panią Prokurator. Znacznym obciążeniem dla organów ścigania są tzw. alarmy „kaskadowe" wysyłane drogą e–mailową. Wspomniano o statystykach dotyczących ewakuacji osób z obiektów. Zaobserwowano znaczny wzrost incydentów związany z mową nienawiści, oszustw związanych z sytuacją covidową, kampanie phishingowe dedykowane pod kwarantannę, czy pod wszelkiego rodzaju dopłaty.

Przestępcy nie zmieniają celu i kierunku swoich działań, ale doskonalą metody i dostosowują je do postępu technologicznego. Rozwój IT dostarcza nowe metody, nowoczesne rozwiązania i środki do popełniania znanych przestępstw w nowym stylu. Obecnie nawet w reklamach telewizyjnych pokazywane są i zachwalane wszelkiego rodzaju usługi anonimizacyjne. Policja na przestrzeni ostatnich lat ewoluuje w kierunku zwiększenia możliwości ścigania cyberprzestępczości. W tym celu zostały wyodrębnione wyspecjalizowane struktury w postaci wydziałów do walki z cyberprzestępczością w komendach wojewódzkich i stołecznej. Wydziały te podlegają komendantom wojewódzkim (i stołecznemu), nie podlegają pod Biuro, ma ono wpływ jedynie na decyzje merytoryczne.

Dużym problemem jest zbyt mała liczba funkcjonariuszy procesowych. Przy tak narastającej liczbie spraw jest to kropla w morzu potrzeb. Pan Dyrektor wskazał, że Policja boryka się z ogromną skalą trudności w doborze ludzi. Biuro i ogólnie Policja stanowi zaplecze dla innych służb. Boryka się ze stałym zjawiskiem podbierania sobie funkcjonariuszy przez inne, lepiej

płatne służby. Projekt ustawy CBZC odpowiada potrzebom Policji. Jest pilotowany przez MSWiA i cały czas pozostaje w fazie uzgodnień.

Stworzono nieetatowych koordynatorów w jednostkach szczebla powiatowego, miejskiego i komend rejonowych dla lepszej koordynacji spraw z zakresu cyber. Przygotowano listę koordynatorów nieetatowych m.in. pod powstanie nowych struktur. Obecnie trwa oczekiwanie na wejście tego projektu pod głosowanie. Wskazano, że taka służba jest Policji potrzebna. Pan Dyrektor wyraził oczekiwanie, że CBZC rozwiąże problem liczby etatów, podległości i finansów. Projekt ustawy o powstaniu CBZC przewiduje dla funkcjonariuszy bezpośrednio zaangażowanych w zwalczanie cyberprzestępczości otrzymanie dodatków służbowych.

Zgodnie z planami na terenie Warszawy ma powstać kompleks policyjny – w pierwszej kolejności ma tam powstać budynek dla CBZC. Obecnie nie jest znany pełnomocnik do tworzenia tego Biura. Pełną zdolność jednostka ma osiągnąć w 2025 r. Pan Dyrektor wyraził nadzieję, że zmiana ustawy o Policji zmieni to, że pion cyber nie będzie już służbą kryminalną nazywaną pionem cyber, lecz służbą zwalczającą cyberprzestępczość.

Pan Dyrektor Mariusz Cichomski przedstawił aktualny stan prac nad projektem ustawy o powołaniu CBZC. Projekt został przyjęty przez Stały Komitet Rady Ministrów, procedura legislacyjna jest na wysokim stopniu zaawansowania. Nie wprowadzona została do niego żadna istotna zmiana z punktu widzenia merytorycznego z drobnym wyjątkiem – przyjęta została uwaga Ministra Sprawiedliwości dot. podważenia proponowanej przez MSWiA zmiany art. 19 a - w skrócie dot. zakupu kontrolowanego i wszystkich innych elementów ujętych w art. 19 a. W związku z przyjęciem przez Stały Komitet RM uwagi Ministerstwa Sprawiedliwości odstąpiono od nowelizacji tego artykułu.

Pan Dyrektor zwrócił uwagę, że projekt obejmuje zmianę art. 19 - w pewien sposób rozszerzany ma być zakres przestępstw wskazanych jako katalogowych do prowadzenia kontroli operacyjnej i do innych uprawnień operacyjnych. Co do kwestii uprawnień to art. 20 zawiera poszerzenie zakresu postępowego dot. tajemnic zawodowych. Z punktu widzenia organizacyjnego CBZC ma być zorganizowane na zasadach CBŚP, czyli docelowo Biuro w KGP, a także wydziały przy komendach wojewódzkich i komendzie stołecznej dedykowane zwalczaniu cyberprzestępczości przestaną istnieć. Na poziomie wojewódzkim powstaną analogicznie jak w przypadku CBŚP wydziały zamiejscowe.

Pan Dyrektor zwrócił uwagę, że poza zadaniami nałożonymi na nowo powstającą jednolitą w skali kraju jednostkę organizacyjną Policji, do zadań należy także wsparcie innych jednostek Policji. Pan Dyrektor wskazał, że termin 1 stycznia 2022 r. jako termin rozpoczęcia funkcjonowania pełnomocnika CBZC jest realny.

Pani Prokurator wyraziła aprobatę z poszerzenia katalogu z art. 19, natomiast zwróciła uwagę, że z katalogu został usunięty art. 267, czyli hacking komputerowy, który był tam w wersji ustawy pierwotnej z lipca br. Projekt ma się odnosić do zwiększenia skuteczności zwalczania cyberprzestępczości, natomiast w art. 19a mowa jest o możliwości zakupu

przedmiotu. Jest to problem na gruncie prawa karnego i postępowania karnego, bo dane nie są rzeczą.

Pojawiło się pytanie, czy nie należałoby rozważyć dostosowania przepisów dotyczących czynności operacyjnych do pracy wykonywanej przez funkcjonariuszy pionów cyber, ponieważ w kolejnych iteracjach projektu usunięto również art. 19 c. Zastanawiano się czy podczas prac nad projektem można byłoby ewentualnie rozważyć dozbrojenie wydziałów cyber w możliwości i narzędzia zachowujące gwarancje procesowe i szanujące prywatność użytkowników, których dane są pozyskiwane.

Pan Dyrektor M. Cichomski wskazał, że art. 267 został usunięty z dwóch powodów – jest to przestępstwo wnioskowe, górna sankcja wynosi 2 lata, co w istotny sposób odbiega od innych przestępstw katalogowych wskazanych w art. 19. Zmiana ta została formalnie zaakceptowana przez Policję. W odniesieniu do art. 19 c pojawił się problem konstrukcji przepisów i jego rzeczywistej niezbędności. Miał on charakter kontratypiczny z punktu widzenia uprawnienia wynikającego z samego art. 19. Pojawiało się pytanie ze strony innych organów uprawnionych do stosowania kontroli operacyjnej czy ten przepis jest niezbędny, czy uprawnieniu musi odpowiadać kontratyp, po to żeby nie popełnić przestępstwa.

Zagadnienie jest podnoszone w wielu aspektach stosowania ustaw pragmatycznych. Mając na uwadze, że tego typu konstrukcja prawna nie występuje również wśród innych organów, które kontrolę operacyjną mogą stosować, realizują działania w cyberprzestrzeni i takich przepisów nie mają oraz nie wskazują na ich niezbędność, ostatecznie podjęto decyzję o rezygnacji z tego przepisu. Pan Dyrektor odnosząc się do możliwości włączenia innych uprawnień do zastosowania mających zawrzeć się w projekcie CBZC wskazał, że projekt jest przed Radą Ministrów oraz sejmowym procesem legislacyjnym, więc takie uprawnienie jest możliwe, jednak MSWiA musiałoby mieć realną propozycję zapisu. W kontekście typu kwalifikowanego odnośnie powiadomień kaskadowych zmiana kodeksowa znalazła się w przepisach ustanawiających CBZC. Głównym podmiotem realizującym działania w tej sferze jest Policja, stąd to powiązanie.

Zauważono, że należałoby dopracować zmiany w zakresie przepisów dot. hackingu komputerowego, który powinien być przepisem bazowym, jednak nim się nie staje ze względu na niskie zagrożenie karne. Problemem, który wzbudził dyskusję jest kwestia wiedzy i umiejętności funkcjonariuszy CBZC oraz kontroli umiejętności z tego zakresu. Pojawiło się pytanie, czy katalog wiedzy i umiejętności z zakresu informatyki i nowoczesnych technologii nie powinien podlegać dalszej ewaluacji, ponieważ nie wszystkie stanowiska takich umiejętności będą wymagać.

Pan Dyrektor M. Cichomski poinformował, że na chwilę obecną procedowana jest zmiana kodeksu karnego, zaostrzane są sankcje oraz dostosowane są do tego pragmatyki. Natomiast, jeśli chodzi o kwestie kwalifikacji, rozporządzenie, które jest załączone do ustawy jako materiał podglądowy, będzie przechodziło konsultacje międzyresortowe i publiczne. Z punktu widzenia kadrowego, nie każdy, kto będzie pracował w CBZC będzie musiał posiadać

wybitną wiedzę w zakresie systemów informatycznych i programowania. Ta wiedza będzie potrzebna wyłącznie na stanowisku z tym ściśle związanym.

Pan Dyrektor S. Szumilas dodał, że w nowych strukturach mają powstać różne wydziały, w których będą inne wymagania, m.in.: wydział zajmujący się analizą sprzętu i oprogramowania, wydział reagowania na incydenty. Podkreślono, że w Policji brakuje osób zatrudnionych na etatach tzw. „dochodzeniowców" w wydziałach Cyber. Zaproponowano, aby wymagania pogrupować i dostosować do pionów.

Jeden z członków Rady wspomniał o nowelizacji Ustawy o Cyberbezpieczeństwie, zawierającej rozdział dotyczący świadczenia teleinformatycznego. Jest to dodatkowe świadczenie przysługujące wszelkiego rodzaju pracownikom, funkcjonariuszom służb, którzy będą realizować określone zadania, w tym związane z cyberbezpieczeństwem.

CBZC przejmie zadania Biura oraz zadania, które są w tej chwili realizowane przez wydziały cyber w Komendach Wojewódzkich. Natomiast osoby się tym zajmujące nie będą przechodziły automatycznie, ponieważ o tym zdecyduje pełnomocnik, który będzie tworzył Biuro. Dodano, że jeżeli zostaną jakieś osoby w strukturach Komend Wojewódzkich, które nie przejdą do tego Biura, a komendanci będą chcieli stworzyć zespół, który będzie funkcjonował w wydziale kryminalnym, dochodzeniowym czy też w technice operacyjnej to taki zespół powstanie. Potwierdzono, że CBZC przejmie zadania i będzie wspierać jednostki terenowe. Postępowania kwalifikacyjne do Policji trwają dłuższy czas. Podkreślono, ze etaty z Policji nie znikają, następuje zwiększenie stanu etatowego ewidencyjnego w Policji o 300 etatów, obecnie istnieje ich ponad 3 tys. Środki w związku z przeniesieniem funkcjonariuszy również pozostają, zatem będzie możliwość zapewnienia ciągłości.

W toku dyskusji Pan Mirosław Maj wyraził wątpliwości. Zasilenie Policji, czy jakiegokolwiek biura, lub też struktury administracji państwowej tak dużą liczbą (1800) wykwalifikowanych specjalistów jest nierealne. Projekt, z punktu widzenia budżetowego, jest drugim największym projektem, jeśli chodzi o cyberbezpieczeństwo w Polsce. To przedsięwzięcie nie ma żadnego odzwierciedlenia w Krajowym Systemie Cyberbezpieczeństwa. Jeżeli zostanie zrealizowane założenie Ustawy i w tej służbie znajdzie się 1800 osób to ten sukces może być katastrofalny w skutkach dla wielu innych aspektów cyberbezpieczeństwa w Polsce. Podkreślono również, że zlikwidowano kierunek nauczania, który miałby dostarczyć specjalistów oraz zakład, który zajmował się edukacją i wzmacnianiem siły kompetencyjnej Policji.

Pan Dyrektor S. Szumilas podkreślił, że Policja nie ma takiego zaplecza jak MON. Zaznaczył również, że trwają rozmowy na temat powrotu zajęć i kształcenia funkcjonariuszy w kierunku cyberbezpieczeństwa.

Jeden z członków Rady zaproponował, aby dobrze zastanowić się nad brakami kadrowymi. Kwestia osób przygotowanych do działania w obszarze cyberbezpieczeństwa jest najsłabszą częścią wszystkich działań, jakie są podejmowane, a synchronizacja tego z Ustawą o Krajowym Systemie Cyberbezpieczeństwa ma zasadnicze znaczenie. Gdy wejdzie ona w życie

wraz z Dyrektywą NIS 2 to będzie konieczna budowa w dużej części gospodarki i administracji publicznej Security Operations Center. Należy przekazywać te informacje, oczekiwane są duże liczby specjalistów i ekspertów w tym zakresie. Członek Rady podkreślił, że nie widzi zsynchronizowanych działań w obszarze kształcenia i edukacji na tę skalę. W tej chwili zostały do Ogólnopolskich Ram Kwalifikacji wpisane trzy certyfikaty w zakresie cyberbezpieczeństwa, które mają potwierdzać wiedzę i umiejętności.

Pan Mirosław Maj dodał, że po wprowadzeniu nowelizacji, kilkanaście organów właściwych w Polsce obowiązkowo będzie musiało powołać CSIRT sektorowe. Z obliczeń wynika, że do uruchomienia takiego ośrodka potrzeba kilkudziesięciu specjalistów. Przy wprowadzeniu nowelizacji każdy z operatorów usług kluczowych będzie potrzebował specjalistów, którzy są niezbędni do pracy w Security Operations Center.

Podczas dyskusji wspomniano, że uczelnie starają się dostosować do braków kadrowych. Na Politechnice Poznańskiej od marca 2022 r. rusza program magisterski w języku angielskim, ale nie da się zbudować zaplecza laboratoryjnego i znaleźć fachowców, którzy mają za zadanie przekazać specjalistyczną wiedzę. Politechnika Poznańska, w celu rozwiązania tego problemu współpracuje z ośrodkami zagranicznymi.

Przedstawiciel MSWiA odniósł się do spraw kadrowych. Przekazał, że poszukiwane są rozwiązania, aby maksymalnie opóźnić odchodzenie na emeryturę ludzi w średnim wieku, dobrze doświadczonych. Temu miało służyć wprowadzenie w zeszłym roku świadczenia motywującego. W kontekście kosztów szkoleń, zostały zmienione określenia zasad spisywania umów, które mają na celu spowolnić proces odchodzenia specjalistów.

Jeden z członków Rady dodał, że obok myślenia o budowaniu zasobów ludzkich należy zwrócić uwagę na budowanie zdolności technologicznych. Pojawiło się pytanie czy CBZC w swoich założeniach ma odpowiadać na zagrożenia publicznie znane jako APT czy tylko z dziedziny cyberprzestępczości. Pan Dyrektor M. Cichomski odpowiedział, że zakres zadań postawionych przed Policją nie zmienia się. Brak jest w planach rozszerzenia czy w inny sposób definiowana zadań policyjnych. W specjalnych przypadkach sposób prowadzenia postępowania będzie wynikiem innego procesu decyzyjnego.

Pan Przewodniczący zakomunikował, że konieczne jest utworzenie stanowiska Rady w sprawie powołania CBZC, a być może także w sprawie agencji czy innego organu rządowego zajmującego się cyberbezpieczeństwem.

Uczestnicy posiedzenia:

Członkowie Rady:

1. Izabela Albrycht
2. Andrzej Dulka
3. Agnieszka Gryszczyńska
4. Michał Kanownik
5. Janusz Kosiński
6. Mirosław Maj
7. Dariusz Milka
8. Aleksandra Musielak
9. Józef Orzeł - Przewodniczący
10. Bolesław Piasecki
11. Paweł Śniatała
12. Robert Trętowski
13. Mateusz Tykierko
14. Marcin Zarzecki

Zaproszeni goście:

15. Insp. Sławomir Szumilas, Zastępca Dyrektora Biura do walki z cyberprzestępczością Komendy Głównej Policji
16. Mariusz Cichomski, Dyrektor Departamentu Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji
17. Wiesław Paluszyński, ekspert Rady
18. Przemysław Sypniewski, ekspert Rady

Sekretariat Rady i pracownicy Kancelarii Prezesa Rady Ministrów:

19. Anna Biała, Zastępca Dyrektora Departamentu Rozwiązań Innowacyjnych w KPRM
20. Ewa Świętochowska, Ekspertka, Departament Rozwiązań Innowacyjnych w KPRM
21. Krzysztof Głomb, Pełnomocnik Ministra Cyfryzacji do spraw współpracy z administracją samorządową Rzeczpospolitej Polskiej
22. Piotr Rutkowski, doradca do spraw polityki DLT/Blockchain, Departament Architektury Informacyjnej Państwa w KPRM
23. Katarzyna Staromłyńska-Gójska, KPRM

24. Anna Supeł, KPRM
25. Joanna Laskowska, KPRM