Posiedzenie zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa, 3 września 2019 r. godz. 13.30, Sejm, budynek U, sala 04A.

Temat:
Po co CBA narzędzie totalnej inwigilacji?

Gość:
Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW, w latach 2011-2015 członek Rady Konsultacyjnej w CBA.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dzień dobry, witam państwa bardzo serdecznie na kolejnym posiedzeniu zespołu Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa, zespołu śledczego.

Dzisiaj zajmiemy się sprawą „Pegasusa". Zaprosiliśmy pana pułkownika Grzegorza Reszkę. Pan pułkownik był niegdyś szefem Służby Kontrwywiadu Wojskowego, później pracował dla CBA.

Bardzo chcielibyśmy się dowiedzieć tak naprawdę, czy ten Pegasus jest? Wiemy, w przestrzeni publicznej jest informacja na temat tego, że Polska zakupiła ten system, się pojawił jakiś czas temu. Rząd temu nie zaprzecza. Poszczególni politycy PiS-u nie zaprzeczają, że ten Pegasus został zakupiony. Mamy świadomość tego, że jest dosyć doskonałym systemem pozwalającym inwigilować ludzi.

Ale zacznijmy panie pułkowniku od podstawowej rzeczy, od pytania, czym jest ten system i czy rzeczywiście mamy się czego obawiać?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Pracowałem dla CBA w takim znaczeniu pani poseł, że byłem członkiem Rady Konsultacyjnej przy szefie CBA.

Otóż system „Pegasus", o którym pani poseł wspomniała i który tak mocno zelektryzował opinię publiczną, jest systemem szpiegowskim.

Jest mówiąc najogólniej systemem umożliwiającym całkowity wgląd w system operacyjny i kontrolę systemu operacyjnego stosowanego w smartfonach. I to nie jest istotne, czy mówimy o systemie operacyjnym Ios, czy mówimy o systemie android. Daje możliwość kontroli nie tyle wyrywkowej, ale całkowitej kontroli. Ale również daje możliwość aktywnego wykorzystania istniejących

funkcji w danym systemie dla pozyskiwania informacji przez użytkownika tego systemu.

Ten system funkcjonujący w obiegu publicznym pod nazwą, pod kryptonimem „Pegasus", przez niektóre korporacje informatyczne, przez specjalistów w tej dziedzinie, został nazwany bronią. Jest traktowany jako broń. Służy do agresywnego, aktywnego, nie tylko pozyskiwania informacji, ale również informacji, które znajdują się na urządzeniu, czyli na telefonie, ale daje możliwość rozszerzonych funkcji, to znaczy daje możliwości kontrolowania aktywności użytkownika teflonu. Bo istnieje możliwość włączenia kamery, włączenia mikrofonu w trakcie spotkania użytkownika tego telefonu, czyli tak de facto jego funkcjonalność jest rozszerzona i odnośnie nie tylko do użytkownika danego urządzenia.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Czyli, jak rozumiem, ja posiadając ten telefon, mogę być narażona na to, że ktoś nie tylko wykorzysta wszystkie te dane, które w tym telefonie się znajdują, ale może też również potraktować jako urządzenie nagrywające, robiące zdjęcia i co jeszcze? Co jeszcze może się wydarzyć?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Filmujące, w zasadzie wszystko, w zasadzie wszystko. Ja powiem tak, ulegamy takiej złudzie bezpieczeństwa, że oto posługujemy się systemami szyfrującymi. Rozmawialiśmy o tym przed rozpoczęciem posiedzenia tego zespołu. Mamy urządzenia, mamy zamontowane różne aplikacje, systemy bezpieczeństwa, których producent informuje nas uniemożliwiają wgląd w to, co robimy, co piszemy, co mówimy.

Otóż system „Pegasus" jest niebywale inteligentną bronią i posługujmy się taką terminologią, bo to jest broń cybernetyczna. System „Pegasus" czyni, że, czyni iluzją to nasze przeświadczenie o tym, że jesteśmy bezpiecznymi użytkownikami.

Posiada dwie funkcje ten system: po pierwsze - przechwytuje rozmowy audio, które są szyfrowane. Ma taką możliwość, ponieważ przechwytuje teksty wypowiedziane przez użytkownika, wypowiedziane do telefonu przed jego zaszyfrowaniem. To jest pierwsza rzecz. Druga rzecz – system „Pegasus" ma możliwość rejestrowania i tu chodzi o szyfrowanie wiadomości tekstowych. System „Pegasus" łamie te bariery, ponieważ ma w swoich możliwościach taką

oto funkcjonalność, że rejestruje aktywność użytkownika, aktywność na klawiszach. Wiec wpisując informację tekstową, która następnie jest szyfrowana, system „Pegasus" rejestruje tekst taki, jaki użytkownik telefonu wpisuje. Drugim filtrem stonowanym przez „Pegasusa" jest to, że on, jeżeli jest zainstalowany na telefonie, na smartfonie odbiorcy takiej informacji, po jej rozszyfrowaniu, ma dostęp do wersji rozszyfrowanej.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: A czy ja, jako użytkownik tego telefonu, mam jakąkolwiek szansę dowiedzenia się, że ktoś próbował go wykorzystać w taki sposób?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Gdyby pani poszła do informatyka, gdyby pani poszła do specjalisty w tej dziedzinie, nie ma pani możliwości, ma pani bardzo niewielkie możliwości dowiedzenia się, że ten system został pani zainstalowany.

Ponieważ jest to system, który, trzeba by tutaj troszkę wrócić. Otóż to jest system, który de facto, według części informatyków, jest użytkowany docelowo. To znaczy, abonent telefonu, urządzenia, na którym jest zainstalowany, jest wybierany, nie jest przypadkowy.

System „Pegasus" ma możliwość autodestrukcji i samolikwidacji w zasadzie w dwóch możliwych przypadkach.

Po pierwsze, wtedy, kiedy wykryje aktywne działanie oprogramowania, które mówiąc najogólniej i wprost, może mu zaszkodzić, to znaczy zablokować jego działanie, bądź może go dezaktywować. To jest jedna rzecz. Druga rzecz – dezaktywuje się według część informatyków, w momencie, kiedy w ciągu 60 dni nie może nawiązać kontaktu z serwerem, który, nazwijmy, jest serwerem dowodzenia, z którego jest zadaniowane. I trzecia rzecz – dezaktywuje się po stwierdzeniu, że został omyłkowo zainstalowany na urządzeniu. Znaczy omyłkowo, w tym sensie, że odczytuje dane z karty sim i jeśli uzna, że tutaj nastąpiła pomyłka, następuje autodestrukcja i wycofanie się systemu „Pegasus" z urządzenia.

Jest inny sposób dowiedzenia się tego, czy system został zamontowany na telefonie. Moment ujawnienia informacji, które były poufne, które pani komuś przekazała i moment, w którym zostały one upublicznione.

Są bardzo niewielkie możliwości i szanse na to, żeby stwierdzić, że ten system został zainstalowany według, według ustaleń informatyków. Najlepszym

dowodem na to jest to, że ten system tak funkcjonuje, to że Apple, który instaluje oprogramowanie na swoich urządzeniach, zainstalował łatki, które miały teoretycznie zablokować działanie tego systemu „Pegasus". Dopiero po medialnych informacjach, które dotyczyły użycia „Pegasusa", kończyły się tragicznie. Tzn. kończyły się albo aresztowaniami osób działającymi na rzecz praw obywatelskich albo, tak, jak w przypadku nieżyjącego dziennikarza Chaszodżdżiego, którego użytkownicy zostali zamordowani.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Cezary Tomczyk.

Cezary Tomczyk, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Szanowni państwo, w polskim prawie jest tak, że, żeby móc kogoś podsłuchiwać, trzeba mieć na to pozwolenie sądu. I ta procedura jest ściśle określona prawem, dlatego, że jest ona wyjątkowa i tylko w wyjątkowych okolicznościach może być stosowana.

Czyli to, co pan przedstawia, pokazuje raczej obraz czegoś odwrotnego, czegoś, co jest na drugim biegunie. Czegoś, co jest narzędziem, z którego korzystają służby, ale jednak bez uprzedniej zgody sądu. Dlatego, że o ile podsłuch dotyczy rozmów, to tutaj mówimy o właściwie całości korespondencji. Mówimy o aktywności, o śledzeniu tego człowieka i ten system może być użyty wobec de facto każdego obywatela w Polsce. To jest jakby pierwsza rzecz i komentarz.

I druga sprawa, my musimy pamiętać, że w latach 2005-2007, wtedy, kiedy trwał rząd PiS-u i kiedy wiceszefem Centralnego Biura Antykorupcyjnego był pan Wąsik, który dzisiaj jest zastępcą Mariusza Kamińskiego w randze sekretarza stanu i zajmuje się polskimi służbami specjalnymi, to właśnie w siedzibie Centralnego Biura Antykorupcyjnego został zamontowany system, gdzie online pan Wśsik mógł podsłuchiwać każdego, kogo CBA aktualnie śledziło. I nie dotyczyło to tylko rozpracowania przestępców. Chodziło również o polityków. Wiemy, że śledzony był chociażby pan prezydenta Aleksander Kwaśniewski.

Z informacji, które zostały ujawnione przez media, okazało się, że pan Wąsik podsłuchiwał polskich obywateli ponad 6. tysięcy razy. 6 tysięcy razy w ciągu dwóch lat! Niech to pokaże skalę paranoi tego rządu i tego, do czego jest zdolny. Ci ludzie często, jak pan Mariusz Kamiński i jego współpracownicy, zostali skazani za przekroczenie uprawnień lub niedopełnienie obowiązków w

związku z tym, co robili z polskimi służbami specjalnymi i co robili w resortach siłowych.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Pełna zgoda. Jeśli mógłbym odnieść się do tego, co pan poseł powiedział, zacząłbym od końca.

Jeśli jest coś, za co podziwiam, jeśli można tak powiedzieć, podziwiam pana Wąsika, a mówię to z perspektywy byłego funkcjonariusza kontrwywiadu i później, czy szefa i pracownika, współpracownika CBA w charakterze członka rady konsultacyjnej. Jeśli jest coś, za co go podziwiam to to, że poświęcił tyle czasu i osobiście odsłuchiwał informacje, odsłuchiwał to znaczy osobiście był zaangażowany w odsłuch podsłuchiwanych rozmów telefonicznych. To jest czynność niebywale mozolna, czasochłonna i mówiąc wprost, mówię to jako funkcjonariusz z pełnym szacunkiem do pracowników pionu techniki, którzy się tym zajmują, jest to nudne.

Ale wskazanie, że pan Wąsik osobiście był w to zaangażowany, inaczej, osobiste zaangażowanie pana Wąsika w te czynności wskazuje, że pana Wąsika, jako zastępy szefa CBA, nie interesowały być może jakieś rzeczywiste działania przestępcze, co być może działania, które mogły być wykorzystywane w jakiś innych celach. Jest bardzo wiele niejasności co do tego, dlaczego pan Wąsik się tym zajmował? Ale to tyle dygresji ogólnej.

Ale ja bym chciał wrócić do początku pańskiej wypowiedzi panie pośle. Otóż tak w istocie jest. Podsłuch i powiedzmy używanie terminu podsłuch, jako takiego wspólnego terminu na podsłuch i podgląd. Bo istnieją oczywiście możliwości techniczne, by legalnie, a jak się okazuje również nielegalnie, uzyskać wgląd w korespondencję mailową przesyłaną pocztą. Więc generalnie stosujmy terminologię podsłuch.

Otóż tak, uzyskanie zgody przez służby specjalne na stosowanie tego narzędzia, jest poprzedzone dość żmudną procedurą. To znaczy, po pierwsze – że to nie jest tak, nie dzieje się tak, że oficer operacyjny prowadzący jakaś sprawę uznaje, że dobrze, w porządku, teraz powinienem uzupełnić brakującą wiedzę dotyczącą aktywności osoby rozpoznawalnej i włączę podsłuch.

Z wnioskiem o zainstalowanie tego narzędzia, zastosowanie tego narzędzia, należy jak prokuratura zgłosić się do sądu. Sąd podejmuje decyzję. Czy jest zasadne, czy nie jest zasadne stosowanie tego narzędzia. I nie znam sprawy operacyjnej, w której sąd zgodziłby się zastosować takie narzędzie na

uzasadnienie, że brakuje nam jakiś informacji. To naprawdę musi być bardzo dobrze udokumentowana sprawa, w której prawdopodobieństwo popełnionego, czy popełnienia czynu karalnego, no, jest bardzo wysokie. To jest po pierwsze.

Po drugie, to, że sąd decyduje o użyciu tego narzędzia, to jest pewna gwarancja, gwarancja tego, że narzędzie to będzie stosowane zgodnie z procedurą i trybem przewidzianym przez prawo. I to jest pierwsza, pierwszy filtr, który chroni obywateli.

Drugi jest zupełnie nieoczekiwany. Dlatego, że przy tego typu procedurze, drugim filtrem jest operator. Bo funkcjonariusz, służba, która uzyska zgodę na stosowanie tego narzędzia, następnie udaje się do operatora. I tam następuje cały ten cykl techniczny, nie będę teraz w szczegóły wchodził, polegający na uruchomieniu tego podsłuchu i korzystania z tego narzędzia. Jeśli jest jakaś sytuacja, zdarzają się takie sytuacje, że trzeba działać szybko, niezwłocznie, to i tak służba musi uzyskać zgodę następczą. 30 dni zdaje się, od momentu zakończenia stosowania tego narzędzia, musi udać się do sądu i uzyskać tzw. zgodę następczą.

Tu rodzi się zasadnicze pytanie przy systemie „Pegasus”. Bo jeśli jest tak, jak donoszą media, że dysponentem tego narzędzia jest służba, no bo nie spotkaliśmy się z informacją, że dysponentem jakikolwiek operator. Służba nabyła prawdopodobnie to narzędzie. Nabyła go nie po to aby obdarzyć prywatnych operatorów. Więc jeśli dysponentem tego narzędzia, tego systemu, jest służba, to automatycznie zostały zlikwidowane, automatycznie zostały zlikwidowane te dwie bariery, które są równocześnie filtrem, co do legalności użycia podsłuchu.

Nie ma sądu i nie ma operatora. Sądem jest tutaj wola szefa, drugim filtrem jest również wola szefa. Jeśli tak jest, to jest to skandal niebywały.

Ja państwu powiem tak, ja byłem funkcjonariuszem w służbach i pełniłem funkcje analityczne, byłem oficerem operacyjnym. Oczywiście można ulec pokusie stosowania narzędzia w sposób niezgodny z prawem. Ale tylko wtedy ulega się tej pokusie, kiedy za nic, w sposób, ale absolutnie za nic, posiada się jakiekolwiek elementarne normy prawne.

W tej chwili sytuację mamy taką – po znowelizowaniu prawa karnego, dopuszcza się dowody użyte w sposób nielegalny. Przedtem było tak, jeśli u kogokolwiek zrodziła się, zrodził się pomysł użycia w sposób nielegalny tego

typu narzędzia, to i tak miał pełną świadomość, że po pierwsze, ujawniając to podlega karze za przekroczenie uprawnień. A po drugie, ten dowód, który by uzyskał w ten sposób z mocy prawa jest nieważny, nieistotny. Jest dowodem, owszem, ale na popełnienie przestępstwa przez funkcjonariusza.

Z informacji, które są dostępne w mediach, z wypowiedzi informatyków, którzy zajmują się tego typu oprogramowaniem, wynika w sposób jednoznaczny, że oprogramowanie to jest używane nie przez operatorów, ale poprzez służby. Mamy tego też dowody empiryczne. Przez służby na razie nie udowodniliśmy. Mamy dowody pośrednie. Bardzo wyraźnie wskazujące na to, że być może CBA zostało w ten proces włączony. Ale mamy dowody z państw innych niż Polska, że ten system działa i był w dyspozycji służb. Ale akurat to nie jest przyjemne dla nas. W służbach państw, które swobody obywatelskie mają w dalszej kolejności, jeżeli chodzi o priorytety funkcjonowania.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Pan Siemoniak.

Tomasz Siemoniak, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Po tym, co pan pułkownik powiedział, nie ma wielkich wątpliwości, co do tego, że jeśli informacje mediów o tym, że taki system został kupiony, a one są bardzo uprawdopodobnione różnymi zagranicznymi doniesieniami, są po prostu łamaniem prawa na bezprecedensową skalę, która tutaj nie ma analogii chyba w trzydziestu latach historii po 89’ roku.

I chciałbym w związku z tym zapytać pana pułkownika, jako osobę, która też kierowała służbom, która zna mechanizm podejmowania pewnych decyzji i też mając własne doświadczenia jako minister obrony narodowej, zasiadania w kolegium służb specjalnych, wiedząc, w jaki sposób pewne decyzje są podejmowane, czy pańskim zdaniem jest możliwe, żeby o zakupie takiego systemu nie wiedział premier, prezydent, ministrowie, członkowie kolegium służb specjalnych?

Trudno sobie wyobrazić, że tego rodzaju zakup miałby być jednie decyzją szefa konkretnej służby. Służby zresztą, która jeśli już uznawać, że takie systemy są stosowane przeciwko terrorystom, zagrożeniom terrorystycznym, akurat zagrożeniami terrorystycznymi się nie zajmuje. CBA się zajmuje zupełnie innymi sprawami.

Więc pytam, jak pan to ocenia? Bo według mojej intuicji, według mojej wiedzy, to jest po prostu niemożliwe i ja sobie nie wyobrażam w czasach, kiedy obserwowałem działanie służb, żeby szef służby bez akceptacji ministra, koordynatora, czy premiera, podejmował takie decyzje. Bo to by oznaczało, że nad służbami specjalnymi nie ma po prostu cywilnej, politycznej kontroli.

Bo to narzędzie, o którym rozmawiamy, według tego opisu, który pan pułkownik nam przedstawił, tak samo może służyć do inwigilowania polityków własnego obozu, czy dziennikarzy własnego obozu. I tu nie ma żadnego ograniczenia.

W zawiązku z tym pytanie o odpowiedzialność polityków, bo jeśli wiedzieli o tym, to myślę, że tutaj jakieś najpoważniejsze kategorie odpowiedzialności, czy przed sądem, czy przed Trybunałem Stanu wchodzą w grę, bo mamy do czynienia z jaskrawym złamaniem prawa.

Bo nie trzeba tutaj jakieś wielkiej domyślności, żeby dojść do tego, przeciwko komu taki system w warunkach polskich jest używany. Gdzie terroryzm na szczęście jest na bardzo małą skalę lub prawie go nie ma. Nie ma takich zagrożeń, do których trzeba używać nadzwyczajnych narzędzi, wiec siłą rzeczy dziennikarze, krytyczni wobec władzy i politycy opozycji wydają się naturalnym celem tego rodzaju systemu.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Absolutnie zgadzam się z hipotezami, które pan poseł postawił, to znaczy również nie mieści mi się w głowie, by zakup takiego sprzętu mógł być przeprowadzony przez szefa służby bez wiedzy nadzorującego go ministra, bez wiedzy premiera. Tu nie ma dobrej odpowiedzi dla ministra Kamińskiego ani premiera Morawieckiego.

Obserwuję to, co się dzieje w służbach, to, co się dzieje wokół służb. Jestem zaniepokojony nie tylko tym, co się dzieje w środku, ale również podejściem do wykonywania zadań przez te służby. W rankingu szefów stosuje się terminologię, kto jest mocnym, a kto jest słabym szefem. Mocnym szefem jest ten, kogo lubi minister Kamiński, słabym szefem jest ten, kogo minister Kamiński nie bardzo lubi. A są tacy wśród szefów i zastępców szefa. Szef Bejda jest jednym z najbardziej zaufanych szefów ministra Kamińskiego. Ale zaufanie szefa Kamińskiego jest akurat dla mnie powodem totalnego braku zaufania. Dowody na to mamy i z lat 2005–2007 i z lat obecnych.

Szefowie służb dość, powiedziałbym, romantycznie podchodzą do ustaw regulujących działanie służb. Jeżeli szef Agencji Bezpieczeństwa Wewnętrznego ze spokojna twarzą, z kamiennym obliczem, informuje opinię publiczną, iż ABW nie zajmuje się spółkami prywatnymi, a udziela takiej odpowiedzi w kontekście działań podjętych przez ABW w przypadku spółki „Srebrna", to ja nie mam żadnych wielkich oczekiwań wobec szefa Pogonowskiego. Mógłbym powiedzieć, że każdy dzień szefa Pogonowskiego na jego stanowisku jest jego prywatnym sukcesem. Ale to nie jest sukces tej służby i to nie jest sukces nas, jako obywateli państwa polskiego.

Jeżeli szef Bejda, w odpowiedzi na pytanie dziennikarza, mówi, że nie zajmuje się sprawami technicznymi i odsyła do rzecznika prasowego, odpowiadając na pytanie o „Pegasusa", to jest taki klasyczny unik. Możemy się bawić w takie bon moty, możemy się bawić w takie uniki, a poziom braku bezpieczeństwa będzie rósł.

Więc, reasumując, w moim najgłębszym przekonaniu nawet wśród bardzo mocnych, cieszących się dużym poparciem ministra Kamińskiego, funkcjonariuszy służb specjalnych w Polsce nie mogło powstać wrażenie ani pewność, że zakupu tego można dokonać bez konsultacji i bez zgody. To jest po pierwsze.

Po drugie, jeśli było to konsultowane z ministrem Kamińskim, to nie sądzę, iż taka mocna pozycja ministra Kamińskiego, w strukturach PiS-u była wystarczającym uzasadnieniem tego, by nie poinformować, choćby zdawkowo, premiera Morawieckiego. I to jest tak, jak pan poseł powiedział, jeśli wiedzieli, że ten sprzęt zostanie, ta, powiedzmy platforma, ten system, zostanie zakupiony i udzielili na to zgody, to należy bardzo starannie rozliczyć z tej zgody i z tego zakupu i premiera, i ministra, i szefów. Jeśli natomiast nie wiedział albo będą się tłumaczyć, że nie wiedzieli, to jest to koronny dowód na to, że kompletnie nie panowali nad służbami.

Jest jeszcze coś, o czym nie mówimy i nie powiedzieliśmy do tej pory w debacie o „Pegasusie" albo co nie… co nie brzmiało w sposób, w sposób wystarczający. Otóż ja jestem byłym oficerem kontrwywiadu. Słysząc i zapoznając się z materiałami dotyczącymi „Pegasusa" zadałem sobie pytanie, kto korzysta z tych informacji? Oczywistym dla mnie faktem jest to, że oczywiście ci, którzy zakupili, ci, którzy go zakupili, aby mieć dostęp do informacji, które są w ich polu zainteresowania.

Ale przy tego typu sprzęcie, przy tego typu programach, jest bardzo istotne udzielenie odpowiedzi, czy producent, czyli spółka NSO ma dostęp, czy nie ma dostępu do uzyskiwanych informacji. Mówiąc inaczej, czy podmioty zagraniczne, ja już nie mówię o służbach, czy podmioty zagraniczne biorące udział w produkcji i dystrybucji, przecież to narzędzie udoskonalane to każdy informatyk powie, że w momencie, kiedy zostanie opracowany jakiś program, trwają prace nad rozwinięciem tego programu, to jest praca niekończąca się. Więc nie chcę używać tutaj zwrotów, czy obce wywiady, czy obce podmioty mają do tego dostęp, czy nie.

Spółka NSO jest spółką izraelską. Na swoich stronach i swoich wypowiedziach publicznych pracownicy tej spółki twierdzą, że oprogramowanie to jest sprzedawane tylko i wyłącznie w celu rozpoznawania i zapobiegania terroryzmowi przestępczości, że, i to jest jedna rzecz, do której trzeba będzie wrócić, ja myślę, co do której trzeba będzie zadać pytanie, sprzedaż tego oprogramowania za granicę podmiotom zagranicznym podlega konsultacjom z agencjami, agentami bezpieczeństwa państwa Izrael.

W związku z tym, jak rozumieć wypowiedź publiczną jednego z pracowników spółki NSO? Poinformował, że spółka ta ma możliwość dokonywania audytu wykorzystania oprogramowania. Co to znaczy audyt wykorzystania oprogramowania? Wypowiedź ta pojawiła się po zabójstwie redaktora Chaszodżdżiego. Jeśli tak jest w istocie, to znaczy służba specjalna, jeśli zakupiła to oprogramowanie, która powinna dbać o bezpieczeństwo państwa, tak de facto wprowadziła konia trojańskiego. Bo jeśli pracownik spółki zagranicznej ma możliwość kontroli użytkowania, to znaczy ma możliwość kontroli abonentów, których śledzi program, a jeśli ma taką możliwość, to być może ma możliwość uzyskania wglądu do treść rozmów?

Rodzi się cały szereg pytań. Pytanie podstawowe. Czy oprogramowanie „Pegasus” i sprzęt, bo ja domyślam się, że wraz z oprogramowaniem, bo został zakupiony sprzęt służący infekowaniu smartfonów, służący modyfikowaniu działalności tego oprogramowania, a więc, czy oprogramowanie i sprzęt przeszły akredytację i certyfikację wymaganą polskim prawem?

Dopuszczenie do sprzedaży na rynku polskim jakikolwiek i jakiegokolwiek modelu samochodu już uznanej marki produkującej ten samochód, już samochody od wielu, wielu lat, nie, tutaj obrazowo, wymagają homologacji dla każdej, dla każdego nowego modelu. Sprzęt teleinformatyczny, z racji swojej wrażliwości, inaczej, z racji wrażliwości sfery, której dotyczy, wymaga również

akredytacji i certyfikacji. Władzą krajową bezpieczeństwa w tym kontekście jest Agencja Bezpieczeństwa Wewnętrznego, no i służba kontrwywiadu wojskowego, która wykonuje w odpowiednim segmencie swoje badania i w porozumieniu z szefem ABW, więc ja pytam, czy program „Pegasus" i czy infrastruktura techniczna służąca do użytkowania tego oprogramowania przeszły wymagany prawem proces akredytacji i certyfikacji? Dotyczy to bezpieczeństwa przetwarzanych informacji uzyskiwanych, opracowywanych, gromadzonych przez ten system.

Funkcjonalność tego systemu, jest funkcjonalnością, która zapewnia użytkownikowi programu nieograniczony w zasadzie dostęp do informacji przekazywanych przez to urządzenie, jak również do kontroli aktywności użytkownika. To już nie chodzi tylko i wyłącznie o sam telefon, nie chodzi tylko i wyłącznie o sms-y i nie chodzi tylko i wyłącznie o rozmowy telefoniczne, nie chodzi również o możliwość uruchamiania kamery. To jest pewien produkt, tak ten produkt trafia do rąk odbiorcy, ale przez to uzyskuje się pełną wiedzę o aktywności osób.

To jest głęboka ingerencja w prywatność, ale to jest również możliwość gromadzenia informacji istotnych dla bezpieczeństwa państwa. Ja nie mówię i nie sugeruję, że użytkownicy smartfonów komunikują między sobą informacje niejawne objęte klauzulą tajną. To nie w tym rzecz. System akredytacji, certyfikacji jest jasno określony.

Notabene, rozmawiałem jakiś czas temu niedawno z pułkownikiem Pawłem Białkiem, który zwrócił mi uwagę na jedną rzecz, nowa kadra w służbach specjalnych odcięła się od wyników i osiągnięć swoich poprzedników, często krytykuje osiągnięcia, jeszcze częściej obejmuje zarzutami karnymi byłych szefów. Proszę sobie wyobrazić, że aktualnym dokumentem, który reguluje akredytacje i certyfikacji sprzętu teleinformatycznego, który wisi na stronach internetowych Agencji Bezpieczeństwa Wewnętrznego, jest zarządzenie generała Krzysztofa Bondaryka z 2011 roku. Upłynęło 8 lat, 8 lat to jest w teleinformatyce i w informatyce ocean czasu.

Ale być może szef Pogonowski, twórczo zinterpretował ustawę o ABW i doszedł do wniosku, że bezpieczeństwo teleinformatyczne go też nie interesuje, że on jest bardziej zainteresowany niebezpieczeństwem teleinformatycznym. Generał Krzysztof Bondaryk był autorem, zatwierdził dokument, wisi na stronach ABW, można sobie to sprawdzić, 8 lat minęło.

Mamy „Pegasusa” i mamy zachwycające milczenie szefów i osób odpowiedzialnych w rządzie. Więc niebezpieczeństw i zagrożeń jest znacznie, znacznie więcej. Każdy z użytkowników czuje się zagrożony i słusznie, sądząc, że jego aktywność mailowa, internetowa, towarzyska, jakakolwiek inna może być w sposób niekontrolowany, niezgodny z prawem, z całą mocą trzeba to podkreślić, niezgodny z prawem, poddana kontroli.

I w tym kontekście, doceniając te wszystkie obawy wszystkich nas, należy na spokojnie powiedzieć, że oprócz tych zagrożeń, co do osób fizycznych, rodzą się też niepokojące pytania dotyczące zagrożeń państwa i dostępu do tych informacji, tak jak powiedziałem, przez osoby, podmioty zagraniczne.

Ja nie chcę wchodzić zbyt głęboko w analizę relacji pomiędzy służbami, ale to jest tak, że państwa, służby izraelskie są służbami zaprzyjaźnionymi, partnerskimi, ale panuje - i to nie jest tajemnicą państwową żadną, dlatego spokojnie o tym powiem - pewna zasada, która obowiązuje wszystkie cywilizowane służby. Szanujemy się, współpracujemy, ale się kontrolujemy i sprawdzamy. To nie jest zaufanie bezgraniczne, ja myślę, że nasi partnerzy z obcych służb partnerskich byliby głęboko rozczarowani, gdyby się dowiedzieli, gdyby uzyskali pewność, że nie zajmujemy się i tego typu działalnością, bo to byłoby… to powód braku profesjonalizmu ze strony polskich służb.

Należy jeszcze do czegoś sięgnąć i udzielić odpowiedzi. Czy oprócz tego, że oprogramowanie i sprzęt były, czy nie były akredytowane i certyfikowane, mam absolutne wątpliwości, co do tego, że były, bo jeżeli prawdą jest, jeżeli prawdą jest wypowiedź pracownika spółki NSO, że spółka ma możliwość audytowania na odległość użytkownika programu „Pegasus”, to, to jest warunek sine qua non i podstawowy do tego, aby akredytacji i certyfikacji nie udzielić. Koniec, kropka, nie ma. Nie może być stosowane w zgodzie z polskim prawem oprogramowanie i urządzenia techniczne do przetwarzania informacji z ochrony teleinformatycznej, co do których nie mamy pewności, że jesteśmy jedynym, wyłącznym dysponentem uzyskiwanych informacji.

Tu jest znacznie więcej potencjalnie popełnionych przestępstw przez nabywców. Pomijając również źródło finansowania, na co zwrócił już uwagę, zwróciła uwagę Najwyższa Izba Kontroli i na koniec w tym kontekście, wydaje mi się, że oczywistym jest, że przy nabyciu tego sprzętu, oprócz akredytacji, certyfikacji, sprawdza się funkcjonalności techniczne, sprawdza się bezpieczeństwo teleinformatyczne i te funkcjonalności związane z

bezpieczeństwem, sprawdza się również producentów. To jest zresztą immamentny element takiej procedury.

Tymczasem pojawiają się niepokojące informacje, dotyczące, co do tego, że własność spółki NSO jest dość niejasna. Struktura własności jest dość niejasna. Powiem tak, krąży taki mit, oparty zapewne na prawdzie, na części prawdy, że spółka NSO została założona przez byłych oficerów Mosadu, to jako dowód profesjonalizmu, jako dowód tego, że sprawą zajęli się ludzie, którzy wiedzą, na czym to polega. Z drugiej strony jest drugi mit, że spółka NSO to jest taka spółka garażowa, która od start up-u do biliardowych obrotów doszła.

Naprawdę nie trzeba dużo czasu stracić, zadałem sobie trud, to zajęło mi to 30-40 sekund. Wstukałem w Google nazwę spółki i okazuje się, że właścicielem spółki NSO jest mała spółka amerykańska, mała spółka amerykańska, pod nazwą nawet sobie wynotowałem tę nazwę, już ją znajdę, zaraz, Fransisco Partners.

Ja nie twierdzę, że jedna i druga spółka, właściciele, udziałowcy tych spółek popełniają czyny zabronione na gruncie prawa polskiego, czy na gruncie prawa izraelskiego, czy amerykańskiego, ale chciałbym wiedzieć, chciałbym wiedzieć, a tutaj wszyscy zasłaniają się, którzy mogą udzielić odpowiedzi, zasłaniają się tajemnicą, chciałbym wiedzieć, czy właściciele, producenci, pośrednicy zostali w sposób właściwy sprawdzeni. Czy my możemy tutaj polegać na tylko i wyłącznie deklaracjach pojawiających się w mediach, pojawiających się ze strony pracowników, czy ekspertów spółki NSO, że program jest absolutnie bezpieczny i sprzedawane tylko i wyłącznie w celu rozpoznawania zagrożeń terrorystycznych i zwalczania przestępczości. Tego nie wiemy.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Panie pułkowniku, nie tylko mamy znaczące milczenie szefów służb, co do tego, czy Polska ma ten system, czy nie.

Mamy również coraz większą wiedzę na temat zorganizowanego hejtu w Ministerstwie Sprawiedliwości przy użyciu różnych wrażliwych danych. No tutaj nie trzeba wielkiej wyobraźni, żeby sobie wyobrazić, w jaki sposób ci ludzie, którzy mogą korzystać z tego systemu i chcą go wykorzystać, korzystając z wrażliwych danych, będą mogli to robić.

Grzegorz Furgo następne pytanie, proszę.

Grzegorz Furgo, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Panie pułkowniku, niejasności jest tutaj co niemiara. Pierwsze niejasności to jest, dlaczego w ogóle CAB zakupiło ten system za ogromne pieniądze z dotacji przekazanej przez Ministerstwo Sprawiedliwości i tutaj Najwyższa Izba Kontroli i nawet to podważała. Tym bardziej, że CBA jest instytucją dofinansowaną przez państwo i nie może, nie powinna korzystać z takich dotacji celowych.

Ale mam pytanie, jedno, które mi się nasuwa na myśl. Chciałbym posłuchać pana opinii, a co jest, jeżeli mamy sytuację, że pan prezydent, pan premier, panowie ministrowie, wszyscy wiedzą o zakupie tego systemu. Jak pan by ocenił wtedy tę sytuację?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Tak, to jest jedna z tych takich ewentualności, które trzeba brać pod uwagę. Oczywiście, jeśli jest tak, jeśli jest tak, że prezydent, premier, minister Kamiński wiedzą o zakupie, wiedzieli o zakupie tego sprzętu, tego sprzętu, to w zasadzie panie pośle powinienem powiedzieć, brak słów. Bo używamy terminu skandal, mega skandal, hiper skandal, brakuje słów, żeby, żeby opisać poziom braku odpowiedzialności z jednej strony, a z drugiej strony poziom poczucia bezkarność.

Ale ja bym chciał zwrócić uwagę na jedną rzecz też, nie tak dawno widziałem wypowiedź profesora Andrzeja Zybertowicza, która mnie bardzo zaniepokoiła, który powiedział, że, no cóż, no tak, dwie rzeczy powiedział, istotne. Tak z jednej strony, że służby nie potwierdziły, nie zaprzeczyły, więc jest prawdopodobieństwo, że mają ten sprzęt to prawda. I z drugiej strony powiedział, że służby powinny mieć daleko idące możliwości stosowania różnych narzędzi, środków i powinna być większa kontrola z drugiej strony.

Jako kontrapunkt dla tego ewentualnego zakupu, podał zakup, jaki rzekomo poczynił Paweł Wojtunik, szef CBA za kilkaset tysięcy euro. No to są po pierwsze nieporównywalne kwoty, to jest raz, nie mówmy o tym, nie mam wiedzy, czy było użyte, czy było kupione, czy nie było. Po drugie, funkcjonowanie CBA pod rządami Pawła Wojtunika i w ogóle służb pod rządami szefów za czasów Platformy Obywatelskiej zgoła nie przypominało takiego radosnego łamania uprawnień, łamania ustaw, opowiadania dyrdymał. Nie dlatego mówię, że sam byłem w tym czasie pełniący obowiązki szefa, ale tak po prostu było.

I wracając do profesora Zybertowicza, ja powiem być może niepopularną rzecz wśród funkcjonariuszy, oficerów służb, szefów, służby mają naprawdę, mają dość dobre w Polsce wyposażenie prawne, techniczne do tego, żeby wykonywać ustawowe zadania.

Po co nagrywać tego typu urządzenie, tego typu program? Rodzi się tylko jedna odpowiedź, po to, aby czynić tego typu kontrolę o jakiej mówimy poza wiedzą kogokolwiek oprócz użytkowników. Poza kontrolą sądów, poza kontrolą prokuratury, aby tę kontrolę czynić tylko i wyłącznie na swój polityczny użytek. I to jest tak, jak poseł Siemoniak powiedział, znając temperament polityków PiS i znając ich zamiłowanie do tajności, spisków, do agentury, no na miejscu polityków PiS-u też bym się bał, na miejscu tych, którzy nie są dopuszczeni do klubu, który ma wiedzę i wpływ na użytkowanie tego urządzenia, a wiemy, że ktoś, kto dzisiaj jest w tym kręgu, jutro może być poza tym kręgiem.

Tutaj, wracając do odpowiedzi na to pytanie, które pan zadał, jeśli prezydent i premier o tym wiedzieli, minister, wiedzieli, no to użyję już tego terminu, który był używany, no to mamy skandal. To mamy, to nie to, że to jest powtórka afery Watergate, czegokolwiek, to mamy, mamy naprawdę sytuację kryzysową i to kryzysową pod wieloma względami i to kryzysową nie tylko i wyłącznie w odniesieniu do bezpieczeństwa poszczególnych obywateli Polski, ale również bezpieczeństwa państwa ze względu na brak wiedzy, co do tego, czy tak zwane backup-y, czy kopie zapasowe są tworzone, czy nie i czy online, czy nie, na przykład producenci mogą mieć wpływ i wiedzę, przepraszam, wiedzę, co do tego, kto jest podsłuchiwany i co w danym momencie powiedział, napisał, wysłał.

Grzegorz Furgo, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: W jakich państwach jest stosowany ten system?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Media donosiły o takich przypadkach, jak Turcja, Meksyk, Zjednoczone Emiraty, Pakistan, Izrael, no i Polska. Jest jeszcze kilka państw, podobno Rumunia, to tutaj trudno, trudno podać taką wyczerpującą listę tych państw, dlatego, że w zasadzie z dnia na dzień ta lista się wydłuża, ale o ironio, dominują na tej liście państwa w których prawa i wolności obywatelskie nie stanowią tak, jak to mówiłem wcześniej, nie stanowią problemu dla władz.

Grzegorz Furgo, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: I ostatnie w zasadzie, prosiłbym pana opinię, a jednocześnie zaapelował do mediów. Panie pułkowniku, sądzę, że ta ekipa wie, wszyscy wiedzą o wprowadzeniu tego systemu. Wprowadzono do Polski, jeżeli to jest prawda, atomową broń cybernetyczną. To może być wszystko poza kontrolą. Wydaje mi się, że mamy z dotychczasowych afer chyba największą aferę przed nami, jaka w ogóle może być. Apeluję do mediów, aby tą sprawą się jednak zająć i prowadzić, bo to jest bardzo groźne. Dotyka każdego Polaka. Panie pułkowniku, wiadomo, że od czterech lat rządzi ekipa, która kompletnie nie zwraca uwagę na istniejące prawo, konstytucję, et cetera, et cetera.

Niech mi pan powie, oczywiście pytanie, każdy z nas zna tę odpowiedź, ale ja bym chciał usłyszeć od pana. Po co CBA taka broń atomowa na zwykłego obywatela?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Nie ma żadnego uzasadnienia ustawowego, jeżeli byśmy przyjęli to tak, jak państwo powiedzieli wcześniej, jeżeli byśmy przyjęli taki, takie założenie, a należy go przyjmować, bo jest dość pośrednich dowodów, świadczących o tym, że to oprogramowanie zostało zakupione.

Jeśli zostało zakupione, to nie ma żadnego uzasadnienia, by nabywcą tego oprogramowania i sprzętu było CBA. Nie uzasadniają tego żadne zapisy ustawowe dotyczące zadań realizowanych przez CBA. Druga rzecz, wybór tutaj tej służby to właśnie może polegać na tym, że jest to służba najbardziej znana, najbardziej lubiana, być może ludzie kierujący, kierownictwo tej służby jest najbardziej cenione i cieszy się zaufaniem ze strony ministra Kamińskiego. Ale ja bym tutaj namawiał również do pewnej zmiany w retoryce. Otóż, bo musimy, jeśli, jeśli, jeśli. To prawda, jeśli ten sprzęt został kupiony, to oprogramowanie zostało kupione, to jest to sytuacja absolutnie wykraczająca swoim skandalem poza, poza jakiekolwiek, tak, możliwości interpretacyjne.

Natomiast przyjąłbym jako pewnik, jeśli to oprogramowanie zostało zakupione, zostało zakupione po to, żeby go używać i jeśli jest używane, to na pewno, to nie być może, to na pewno bezpieczeństwo państwa zostało narażone przez nabywców tego sprzętu. I tu chodzi o bezpieczeństwo poszczególnych obywateli, ale również o bezpieczeństwo państwa interpretowane w kategoriach instytucjonalnych, interpretowane jako bezpieczeństwo i suwerenność.

Tracimy wpływ i nie mamy kontroli jako obywatele poprzez Sejm, a nie mamy kontroli, poprzez sądy nie mamy kontroli, poprzez prokuraturę nie mamy kontroli z prostego i podstawowego względu: nabywcą i użytkownikiem tego sprzętu jest służba specjalna, która może funkcjonować w oderwaniu od procedur sądowych przewidzianych na stosowanie techniki operacyjnej, czy podsłuchu. To jest jedna rzecz.

Druga rzecz jest następująca, jeśli ten sprzęt został zakupiony, tracimy poczucie bezpieczeństwa, tracimy możliwość kontroli, ale rodzi się pytanie, czy nie było tak, ja sam niestety w sposób negatywny to odpowiadam sobie na to pytanie, czy pozytywny, przepraszam, czy nie było tak, że w przeszłości ludzie, którzy zajmowali się bezpieczeństwem, a są związani z PiS-em również mieli naprawdę w niewielkim poszanowaniu bezpieczeństwo państwa.

Oczywiście było, profesor Andrzej Zybertowicz jest znanym specjalistą od rozwibrowywania służb. Ja przypomnę państwu, którą kategorię, która wpłynęła po 2007 roku, kiedy PiS przegrał wybory, kiedy główną metodą naprawy działania służb według profesora Zybertowicza czy zespołu, którym kierował, było doprowadzenie do rozwibrowania służb. Na czym to rozwibrowanie miało polegać? Do rozedrgania, wprowadzenia niepewności. Jeśli taki mamy model służb mieć, że mamy rozwibrowane kadry, no to konsekwencje dla bezpieczeństwa są w sposób jasny i oczywisty wiadome.

I jeszcze jedna rzecz, szefowie służb mają, tak jak już to wielokrotnie mówiłem, dość liberalny stosunek do zadań nakładanych na nich przez ustawy. Sami decydują, czy coś jest, czy coś nie jest w ustawie, czy się można zajmować, czy się nie można zajmować. To nie to, że ja nie mam gwarancji. Ja, jako obywatel mający to szczęście, że pełniłem służbę w Urzędzie Ochrony Państwa, w ABW, w Służbie Kontrwywiadu Wojskowego, jako obywatel mam absolutną pewność, co do tego, że jeśli te urządzenia są w dyspozycji tych osób i tych służb w tej chwili, to ja nie mam prawa czuć się bezpieczny i tak jest.

Tu tryb przypuszczający należy odłożyć jako nieadekwatny, jeśli się ma taki stosunek do systemu, do państwa, jako instytucji, do systemu prawa, do sądu, do prokuratury, to naturalną konsekwencją jest to, że służby specjalne są traktowane przez polityków PiS-u jako oręż, jako oręż partii. To taka sytuacja już miała miejsce w Polsce, kiedy służby specjalne były traktowane jako oręż partii, oręż partii i narodu, to mamy adekwatną sytuację w tej chwili do tego.

Grzegorz Furgo, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję bardzo.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Bożena Kamińska.

Bożena Kamińska, członkini zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję bardzo. Panie pułkowniku, rzeczywiście patrząc na tę sytuację ostatnich dni odnośnie doniesień możliwości funkcjonowania tego systemu w naszym kraju, szef CBA, pan Bejda nie zaprzecza temu, wręcz nawet odpowiada, że o kwestiach technicznych to z nim proszę nie rozmawiać, bo on się na tym nie zna, czyli, jeżeli ewidentnie nie ma zaprzeczenia od szefów służb i również rządu, absolutnie mamy prawo tutaj domniemywać, że ten system działa, ponieważ informatycy kanadyjscy, którzy obsługują i pracowali nad tym systemem, potwierdzają, że sygnał jest aktywny od 2017 roku w naszym kraju i do dnia dzisiejszego, że w 2016 został zakupiony i nie ma podstaw, żeby temu nie wierzyć.

Niemniej jednak to, co zostało wcześniej zauważone i pan powiedział, ja również miałam to na uwadze, że my musimy otrzymać odpowiedź, na jakich zasadach i warunkach, i jakie tutaj formy prawne zostały zastosowane, żeby przede wszystkim podjąć decyzję o zakupie tego, jak przebiegała w ogóle forma zakupu takiego sprzętu?

Kto go użytkuje i kto go obsługuje? Bo to ja śmiem twierdzić niestety, że to, co pan tutaj nadmienił, ja mam również takie przeświadczenie, że obce służby obsługują to oprogramowanie, znaczy mają wejście przynajmniej do tych zapisów, co się dzieje na tym oprogramowaniu, bo mam przeświadczenie również takie, że my nie mamy odpowiednio przeszkolonych osób, żeby to oprogramowanie właściwie było przez nich obsługiwane, a jeżeli tak, to gdzie i kiedy takie certyfikaty mogli zdobyć i również uzyskać, żeby to właściwie było obsługiwane?

Kolejne moje pytanie jest w stosunku do pana, jako fachowca i osoby, która pracowała przez wiele lat w służbach kontrwywiadu, dlaczego wcześniej Polska nie myślała o zakupie, czy potrzebowała takiego oprogramowania, żeby to właśnie służby kontrwywiadu mogły posługiwać się takim systemem? Czy te systemy, które wtedy mieliśmy, zupełnie nam wystarczały i dlaczego, jeżeli już podejmujemy takie decyzje o zakupie takiego sprzętu, to kto ma być

wnioskodawcą i od kogo, że tak powiem, zaczyna się ten pierwszy krok decyzyjny? Dziękuję bardzo.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Może zacznę od końca, otóż, jeżeli dana służba jest zainteresowana zakupem jakiegoś sprzętu, który umożliwia bardziej efektywne prowadzenie działań, ona jest inicjatorem, ale to jest cały proces.

Tak to, zakup takiego sprzętu nie odbywa się w półmroku, w piwnicy, oczywiście nie nagłaśnia się tego faktu, ale służba jest inicjatorem, cały ten sprzęt przechodzi akredytację, tak, jak mówiłem, certyfikację, zdobywamy pewność, że jesteśmy jedynymi użytkownikami tej wersji tego sprzętu, podpisujemy umowę na ewentualne modyfikacje, na szkolenia od osób obsługujących, to wszystko jest w pakiecie, ale przede wszystkim utrzymujemy, uzyskujemy pewność, co do tego, że jesteśmy jedynym dysponentem, użytkownikiem i beneficjentem uzyskiwanych wyników pracy jakiegoś sprzętu, ale ja wrócę do tego, co mówiłem.

Jak chodzi o możliwości techniczne, którymi dysponują, dysponują polskie służby, to ja oceniam, że polskie służby były bardzo dobrze zaopatrzone i nie tylko w sprzęt, który pochodził zza granicy, ale również w autorskie rozwiązania. Ja już tutaj dalej nie mogę wchodzić, nie będę wchodził w szczegóły, ale naprawdę tu w tej materii nie było źle. Oczywiście trzeba nadążać za rozwojem technologii, brać udział też w tym procesie rozwoju technologii.

Ale ja bym chciał zwrócić uwagę na jeden podstawowy aspekt, użycie tego sprzętu, tej platformy „Pegasus” w istocie sprowadza się w efektach do tego, żeby uzyskać informacje dotyczące rozmów, to znaczy, żebym ja mógł, jako ten oficer, który użytkuje ten sprzęt, mógł podsłuchać kogoś, zajrzeć w jego maile, sms-y, ale ja te możliwości jako oficer i tak posiadałem przed zakupem tamtego sprzętu, w zgodzie z procedurą.

Zgłaszam się do przełożonego, prowadzę sprawę, idę do prokuratury, formułujemy wniosek o zastosowanie techniki, niezależny sąd ocenia, waloryzuje informacje, które uzyskał i podejmuje decyzję i kolokwialnie stwierdzając mówi: ok, należy się wam, proszę bardzo stosować i - uwaga! - w określonym reżimie, to znaczy od daty, godziny, do daty, godziny, a jeżeli zgoda wygaśnie, to trzeba przyjść z wnioskiem o przedłużenie. To nie jest tak, że służba sobie dowolnie przedłuża, potem w sposób należyty, zgodny z procedurą obchodzić się z uzyskanymi materiałami, włącznie ze zniszczeniem.

Więc zakup tego sprzętu, ja nie rozumiem zakupu tego sprzętu w tym znaczeniu, że pozwala on na uzyskanie nowych możliwości, których służby do tej pory nie miały. Owszem, służby nie miały do tej pory możliwości swobodnego stosowania podsłuchów. Wraz z zakupem tej platformy, tego oprogramowania, służby uzyskały możliwość niekontrolowanego korzystania z podsłuchów, czyli inaczej, niekontrolowanego podsłuchiwania naszych rozmów, przeglądania naszym maili, zawartości, nawet zawartości historycznej, to znaczy wstecz tego, co było nadawane, pisane, przekazywane, co było zrzucane z ekranu, wszystkich screenów.

To jest mega kombajn, nie podlegający kontroli, bo jeszcze raz mówię, przecież służby, jeśli kupiły ten program, to nie po to, żeby wyposażyć w ten program wszystkich operatorów działających na rynku polskim. Jeśli go zakupiły, to po to, żeby go stosować samodzielnie, bez wiedzy, bez zgody sądu, czyli poza trybem przewidzianym przez prawo, no, ale zdaje się już mówiono w Polsce, że coś robię poza trybem i poza innymi regułami, więc pani poseł, tutaj absolutnie ja nie widzę takiej możliwości, bo oczywiście, żeby było jasne, należy rozwijać technologie służące zapewnieniu bezpieczeństwa. Nie należy zaniechać rozpoznawania aktywności terrorystycznej i tak dalej, i tak dalej. To wszystko mamy wpisane w ustawy, służby robią, ale dodatkowo mamy cały pakiet prawa, ustaw, przepisów, które mają chronić nas, jako obywateli.

Pan Mariusz Kamiński, pan Bejda, pan Pogonowski i pan Kowalski, wszyscy szefowie służb, oprócz tego, że są szefami, są też obywatelami. Mnie się wydaje, że u nich w ogóle nie występuje brak podstawowej refleksji polegającej na tym, że oprócz tego, że są generałami, pułkownikami i Bóg wie, kim jeszcze, są zwykłymi obywatelami i to obywatelami, którzy patrzą na swoje zadania i na służby w sposób absolutnie zideologizowany.

I nie mówię tego jako przypuszczenie, formułuję taką ocenę w oparciu o czas, kiedy pełniłem obowiązki szefa Służby Kontrwywiadu Wojskowego po panu pośle Antonim Macierewiczu i obecnym generale Andrzeju Kowalskim, który był pełniącym obowiązki tej służby. To jest absolutne zideologizowanie służb i dzielenie funkcjonariuszy na kategorie. Nasz to mu ufamy, nie nasz to mu nie ufamy. Nie liczą się kategorie profesjonalizmu, kompetencji, doświadczeń, nie, tego nie ma, albo ci ufamy, bo jesteś nasz, albo ci nie ufamy, bo nie jesteś nasz. Nikt nie pyta o kompetencje.

Więc reasumując, wracając do początków. W moim najgłębszym przekonaniu, zakup takiego oprogramowania i sprzętu służącego do obsługi tego

oprogramowania, jeśli miał miejsce, to był motywowany wyłącznie tym, by uzyskać możliwość kontrolowania obywateli poza zgodą, poza trybem sądowym, poza ustawami gwarantującymi bezpieczeństwo i poczucie prywatności. Wszystko inne, to znaczy ryzyka, które stosowanie tego programu niesie dla bezpieczeństwa państwa, to są kwestie, co do których nie sądzę, by sobie panowie zdawali sprawę. Te kwestie ich raczej nie zajmują.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję bardzo. Mam jeszcze trzy osoby zapisane do głosu. Magdalena Kochan.

Magdalena Kochan, członkini zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję bardzo, panie pułkowniku, to, o czym mówimy, jeży włosy na głowie. To jest rzeczywiście bardzo trudne, ale ja chciałam zapytać o coś bardzo osobistego. Pan jest wieloletnim oficerem, dowódcą służb specjalnych, które świateł kamer, które świateł, sceny, kamer, no, nie najchętniej korzystają z tego rodzaju oprzyrządowania.

Chciałam zapytać wprost. Pan, zdając sobie sprawę z tego, co się dzisiaj dzieje w Polsce, dlaczego zdecydował się na rozmowę dzisiaj z nami właśnie w świetle kamer, właśnie wśród dziennikarzy, w rozmowie z opinią publiczną?

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Motywów miałem kilka. Po pierwsze poziom niszczenia instytucji państwa pod rządami obecnego rządu, pod rządami PiS-u osiągnął poziom dla mnie niewyobrażalny.

Ja jestem z wykształcenia socjologiem. Kończyłem socjologie w końcu lat 80-tych w Krakowie. Pracowałem przez kilka lat na uczelni jeszcze w czasach PRL-u i musze pani poseł powiedzieć tak, że nie wyobrażałem sobie w 89-tym roku, nie wyobrażałem sobie po czerwcu 89 roku i później w 90-91r. i następnych latach, nie wyobrażałem sobie, że doczekam takiej sytuacji, w której w sposób jawny, bezczelny, arogancki będą łamane prawa moje, współobywateli, nieważne o jakich poglądach politycznych mówimy. To co się dzieje w tej chwili w państwie polskim, co robi rząd, czemu sprzyja prezydent, jest niszczeniem instytucji państwa.

Przyjdzie nam, jako socjolog to mówię, przyjdzie nam lata pracować nad odbudową zaufania obywateli do państwa i paradoks polega na tym, że w 89-tym roku, w 90-tym roku nie było tak głębokich podziałów, tak wielkiej nieufności, jak w tej chwili.

Paradoks polega też na tym, że można stosować retoryką opartą na całkowitym kłamstwie. Na kłamstwie po prostu i bezczelnie opinii publicznej mówić, że to jest prawda, można łamać prawo mówiąc, że dbamy o przestrzeganie prawa, można łamać prawo mówiąc, że podnieśliśmy praworządność na wyższy poziom. To jest pierwszy motyw.

Drugi motyw zasadniczy jest taki. Ja pracowałem w służbach i wiem doskonale, jak łatwo można zdemoralizować funkcjonariuszy systemem kar, nagród. Specjalistami wysokiej klasy są obecni politycy PiS-u, którzy się zajmują służbami. To jest naprawdę wysoki poziom manipulowania emocjami, manipulowania etatami, awansami, nagrodami. Nie przypuszczałem, że można być dyrektorem pionu operacyjnego w służbie specjalnej, mając praktykę w organizacjach harcerskich tylko i wyłącznie, można doświadczonych oficerów kontrwywiadu instruować co do ich warsztatu pracy.

Jeśli tego typu ludzie o takich intencjach i o takich wynikach, jak chodzi o niszczenie państwa, zabierają się i mówią: robimy drugi krok - będziemy mieli teraz takie urządzenie i takie możliwości, że będziemy kontrolowali w imię oczywiście praworządnych celów, zadań ustawowych, nie podnoszenia bezpieczeństwa państwa i zakupujemy taki sprzęt, będziemy to robić, to już dawno został przekroczony poziom alarmowy, ale w tej chwili, no, nie wypada po prostu powiedzieć niczego.

Nie mogę powiedzieć, że to mnie nie dotyczy. Dotyczy mnie to jako obywatela i to jako osobę, która pełniła funkcję w służbach. Ja naprawdę doskonale jestem w stanie sobie wyobrazić, jaki użytek z tego oprogramowania uczyni te kilka osób, które ma do niego dostęp. Nie wierzę w żadne dobre intencje ani pana Bejdy, ani pana Pogonowskiego, ani pana Kamińskiego i mówię to publicznie. Nie wierzę w żadne intencje, ponieważ ich intencje zostały zweryfikowane przez to, co robili jako ministrowie, jako funkcjonariusze, jako szefowie służb. To tyle.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Elżbieta Radziszewska i później Dorota Niedziela i zmierzamy do końca.

Elżbieta Radziszewska, członkini zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Panie pułkowniku, to, co pan powiedział, to jest coś, co uruchamia wyobraźnię, ale jednocześnie czyni nas

absolutnie bezbronnymi wobec tego, co się może dziać i w Polsce, i poza granicami.

Bo jeśli ten sprzęt jest kupowany z pieniędzy, które miały być przeznaczone na pomoc ofiarom przestępstw z Ministerstwa Sprawiedliwości, gdzie szefem tego ministerstwa jest prokurator generalny, trafiają do służb i mają wykonywać zadania, wykorzystywane przy wykonywaniu zadań, które to do tej służby nie należą, bo ta służba nie ma za cel walki z terroryzmem i właściwie tak naprawdę nie wiadomo, kto tam będzie się tym zajmował. Bo przecież nie szef służby będzie siedział i robił rzeczy techniczne, czy wykonywał polecenia, kogo akurat w tej chwili mamy na tapecie, kogo w tej chwili sprawdzamy.

Więc ilość osób, która może mieć dostęp do tych informacji prywatnych, absolutnie indywidualnych poszczególnych obywateli, ale również tych, które są tajemnicami państwowymi, jest wielu. I niekoniecznie chyba będziemy wiedzieć, w czyich rękach mamy te informacje, pomijając tych, którzy sprawują kontrolę nad oprogramowaniem i nawet nie wiemy gdzie.

Dzisiaj zwykły człowiek mówi: no państwo ma mnie chronić, ale to, co się tam dzieje, jakiś sprzęt kupiono, jest w jednej służbie, co to mnie obchodzi. Tylko, że ludzie nie mają świadomości tego, że za każdym razem to oni mogą być obiektem i może być wykorzystane przeciwko nim, bo już mieliśmy. Teraz ostatnia sprawa związana z sędziami, gdzie z ich akt personalnych, czy z oświadczeń majątkowych wyciągało się to, co mogło im zaszkodzić, bynajmniej nie to, co ich pochwalić, gdzie mieliśmy sytuacje, gdzie protestowali lekarze, młodzi rezydenci i ich prywatne rzeczy nie dość, że ujawniano, to jeszcze przeinaczano, żeby móc w nich uderzyć. Mieliśmy sędziów w ogóle, mieliśmy przedsiębiorców.

Więc pytań do kogo, czy wobec kogo można zastosować sprzęt do tej nielegalnej inwigilacji to można uruchomić wyobraźnię i to może być każdy. Tylko każdy mówi: no dobrze, ale ja nie jestem przedsiębiorcą, nie jestem sędzią, nie jestem lekarzem rezydentem, nie jestem dziennikarzem, nie jestem politykiem partii opozycyjnej, właściwie no jestem jakimś tam małym człowiekiem, ale potem się okazuje, że dochodzi do takiej sytuacji, czego nawet w Polsce PRL-owskiej nie było, że siedzi sobie człowiek na ławce, ma koszulkę na sobie z napisem „konstytucja” i podchodzi policja i nie mając żadnych podstaw do tego, by przypuszczać, że to jest przestępca, czy można go o coś podejrzewać, legitymuje go, żąda wyjaśnień, a jest to aktor w koszulce „konstytucja”.

Czyli ten sprzęt może być wykorzystany w każdej sytuacji, może dotknąć zwykłego człowieka, a że ekipa będzie pomiędzy sobą walczyć, no mieliśmy przykład niedawno, trzy miesiące temu pod postacią pisma, które wystosował do prezydenta Dudy odwołany ambasador „dobrej zmiany" w Japonii, czyli tarcia wewnątrz tej ekipy mogą być też podstawą to tego, żeby sprzęt wykorzystywać.

Nie ma, Rzecznik Praw Obywatelskich dzisiaj jest, który jest, za chwilę będzie inny, ale Rzecznik Praw Obywatelskich przecież wycofał z Trybunału, który nie ma już przecież żadnej władzy prawnej dzisiaj, skargę dotyczącą uwzględnienia dowodów nielegalnie zdobytych przez służby specjalne, tych owoców zatrutego drzewa, gdzie w nowym przepisie wprowadzonym przez tę ekipę, nie dość, że można je wykorzystywać te nielegalne dowody, to jeszcze sąd w wielu przypadkach musi je wykorzystać.

Więc jest pytanie, czy mając na uwadze to co może Pegasus i ten przepis prawa, który jest, to może się okazać, no poza wyjątkami, że funkcjonariusz zamordował kogoś, przepraszam, że trochę ironizuję, ale po prostu można coś zdobyć nielegalnie, czy wykreować coś, przymusić do jakiegoś działania, mieć potem dowody nielegalnie zdobyte i wykorzystać przeciwko komuś nie tylko w Polsce, bo przecież jak tego typu dowody zdobyte przez służbę mogą posłużyć komuś innemu.

Wiemy, że trolle potrafią wpływać na wyniki wyborów, że mogą wpływać na koniunkturę gospodarczą, czy dekoniunkturę, mogą doprowadzać do kryzysu finansowego, więc dzisiaj ta przestępczość w tej cyberprzestrzeni jest rzeczą straszną i sprowadzanie takiego sprzętu bez jakiejkolwiek kontroli prawnej, czy wbrew prawu, jest straszne.

Czy my, panie pułkowniku, jako obywatele, czy my w ogóle możemy mieć nadzieję, że jest jakakolwiek instytucja, instrument prawny w rękach naszych, kto może skontrolować działanie takiego sprzętu i konsekwencje jego wykorzystania? Czy w ogóle cokolwiek, chociaż troszeczkę, my możemy mieć wpływ na kontrolę tego, co się dzieje i może dziać? Dziękuję.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Może od ostatnich kwestii zacznę. Otóż ja jestem umiarkowanym pesymistą, jestem optymistycznie, lekko optymistycznie nastawionym w przyszłość realistą.

To znaczy nie oczekuję, mam pewność, że obecne szefostwo służb, mam tutaj na myśli również pana ministra Kamińskiego, premiera Morawieckiego, nie oczekuję, żeby udzielili prawdziwej miarodajnej odpowiedzi na pytanie, co do tego, czy zostało to zakupione, przez kogo, w jakim celu, jak często i wobec jakich zagrożeń jest użytkowane. Politycy nadzorujący służbę w tej liczbie i premier wielokrotnie dowodzili, że można powiedzieć cokolwiek. Można powiedzieć cokolwiek, a potem się z tego wyplątać mówiąc, że kontekst był inny. Ja bym się nie zdziwił też, gdyby mi ktoś powiedział, że zaprzeczył, że ja tego nie mówiłem, wtedy było inne ciśnienie atmosferyczne, w trakcie takiego ciśnienia właśnie to tak wygląda, a poza tym następne pytanie będzie tak, proszę. Ja nie wierzę politykom PiS-u, którzy kierują służbami. Wielokrotnie nas okłamywali.

Drugi powód, dla których nie wierzę, dla nich kwestia merytorycznej odpowiedzialności za służby nie istnieje. To jest tak, nawiążę tutaj do publicznej wypowiedzi pana Pogonowskiego, który mówił, że służbami, przepraszam spółkami prywatnymi się nie zajmuje ABW. Życzyłbym lektury tej ustawy szefowi Pogonowskiemu, prawnikowi z wykształcenia, zanim takie rzeczy będzie mówił.

Druga kwestia w oparciu której, o którą się tak… mocno będę trzymał tego, że szefowie służb nie cenią profesjonalizmu. To jest kwestia, którą zastałem w Służbie Kontrwywiadu Wojskowego w 2007 roku. Ja, no nie ujawnię jednego zdania, które powiedziałem ministrowi Klichowi, który był ówczesnym ministrem obrony narodowej, po dwóch tygodniach pełnienia przeze mnie funkcji, dlatego że to zabrzmiałoby w tej chwili źle, a być może źle byłoby w ogóle dla służb, ale naprawdę służba generowała wtedy same ryzyka i niebezpieczeństwa. Byliśmy w takiej sytuacji.

Trzecia rzecz. Możliwość użycia tego programu, tego narzędzia jest atrakcyjna z tego względu, że można ją użyć poza procedurą sądową. Poza procedurą sądową, bo legalnie stosowane podsłuchy muszą odbyć tę drogę zatwierdzenia, zgody sądu. Nawet w trybie następczym uzyskane materiały podlegają również określonemu traktowaniu, uzyskane w ten sposób materiały ustawowo o określonym traktowaniu.

Ale jest właśnie to, o czym pani mówiła, pani poseł, znaczy zmiana w kodeksie karnym. Możliwość stosowania dowodów nielegalnie użytych ten przepis w połączeniu z tym narzędziem, z tym oprogramowaniem, daje bardzo duże możliwości do twórczego stosowania możliwości służb specjalnych i możliwości

pracy operacyjnej, co biorąc pod uwagę realne wyniki pracy służb i polityczne zaangażowanie szefów służb, to jest niebywałe, żeby szefowie służb … są politycznie i ideologicznie zaangażowani. Jest to traktowane przez polityków PiS-u jako dowód ich wartości. To jest skandalem.

W połączeniu z tymi możliwościami, które daje znowelizowany kodeks karny i to narzędzie sprawia, że naprawdę nie jest przesadą powiedzenie, że nikt w tym kraju, naszym kochanym kraju, nie może czuć się bezpiecznie. Spokojnie i tajemnica dziennikarska czas przeszły. Tak? Czas przeszły. Tajemnica adwokacka? Czas przeszły. To wszystko odchodzi w przeszłość. Przy bardzo niepewnym moralnie, mówiąc delikatnie, w podejściu do swoich obowiązków szefów służb każe nam się naprawdę bać.

Ja bym zwrócił tutaj uwagę na jeden aspekt. Zauważyłem, że wśród szefów służb i polityków PIS-u występuje taka skłonność stosowania i nadużywania terminu „operacyjny". To jest wyrażenie, którym określa się generalnie sposoby, metody uzyskiwania informacji. Dla polityków PIS i dla kadry kierowniczej służb PIS mam wrażenie, że kategoria wyrażenie „operacyjne" ostatnio służy do retorycznego legalizowania tego, co jest prawnie nielegalne.

Bo jeżeli mi w rozmowie, rozmówca mówi mi: ale wiesz Grzegorz, to jest operacyjne. To jest metoda operacyjna, ale nielegalna, no właśnie operacyjna. No nie jest tak, że wyrażenie „operacyjna" jest synonimem nielegalna. Nie, „operacyjna" służy jako wyrażenie na określenie kilku metod sposobów wykonywania, działań, czynności, niejawnych działań, czynności przez służby specjalne. Co więcej, ten paradoks polega na tym, że te metody są niejawne, a tak naprawdę każdy z nas wie doskonale, bo od czasów biblijnych są one niezmienne w dużej mierze.

Dla PIS-u, oficerów PIS-u, dla szefów służb, kategoria „operacyjne" staje się alibi. To jest słowo klucz, które równocześnie jest zasłoną, to znaczy, jeżeli użyję terminu ok „operacyjne" to zamyka dyskusję. No nie, no nie zamyka dyskusji. To otwiera dyskusję. Jeżeli masz zamiar stosować operacyjnie nielegalne metody to łamiesz prawo. Koniec kropka. Więc, jeżeli jakiś poseł PIS-u mówi, że ja się generalnie na tym nie znam, ale to służby operacyjnie działają, lepiej im zostawić spokój. To to jest alarm ostatniej kategorii.

Operacyjnie to nie znaczy nielegalnie. Operacyjnie to… ekwiwalenty tego są w instrukcjach o pracy operacyjnej, w dokumentach, zarządzeniach wewnętrznych. Jest wszystko szczegółowo wyjaśnione i opisane.

Program ten, program Pegasus został w istocie, jeżeli został zakupiony, to został zakupiony do nielegalnego podsłuchiwania obywateli. Koniec kropka. Nie operacyjnego, nielegalnego.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję. Ostatnie pytanie Dorota Niedziela i prosiłabym, żebyśmy zbliżali się do końca.

Dorota Niedziela, członkini zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Już bardzo krótko. Gdybyśmy byli na spotkaniu literackim i byłaby to pana epicka opowieść o 1984 roku to byłoby to ciekawe.

Natomiast, cały to nasze spotkanie to trochę przerażający horror i ważne jest, żeby bardzo prosto przedstawić społeczeństwu, po co został zakupiony ten system. Do czego on służy? Co to oznacza? A oznacza jedno: chęć pominięcia prawa i nielegalnego, bez jakiegokolwiek nadzoru, podsłuchiwania wszystkich obywateli w Polsce.

Druga sprawa, która mnie zadziwiła to to, że składa się w pewną całość zmiana prawa dopuszczającego te dowody uzyskane w nielegalny sposób z zakupem tego systemu. Co świadczyłoby o tym, że to większy plan na dłuższy czas do zdobycia i ugruntowania swojej władzy i inwigilowania, i walki z opozycją i nie tylko. Z obywatelami, którzy nie są dokładnie tego samego zdania, tej samej partii, której jest władza.

A pytanie. Skoro system ma służyć do obrony obywateli przed terroryzmem, to pytanie, dlaczego, bo nie słyszałam, żeby pan wypowiedział, że jest on zakupiony w USA, dlaczego USA, które generalnie wypowiadają największą wojnę terrorystom, nie mają oficjalnie, jak rozumiem, tego systemu zakupionego? A jeżeli, bo pan powiedział, że tam była spółka, która jest częścią, czy własnością tego Pegasusa zarejestrowana w USA, to pytanie: dlaczego Polska, która nie ma takich doświadczeń, korzysta z tak potężnego narzędzia?

I jeszcze jedno. Czy przedstawione dowody w sprawie, jakieś uzyskane taką drogą, czy mailing, czy sms-y, czy inne dokumenty, nie muszą być opisane w trakcie spraw, że są pozyskane za pomocą tego systemu? Bo to dawałoby jakąkolwiek jeszcze szansę na to, że dowiemy się, czy on był wykorzystywany czy nie. Jeśli nie ma takiego obowiązku, no to nigdy się nie dowiemy, że były, że w 90 procentach było to wykorzystywanie tego nielegalnego systemu.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Zacznę od końca. Otóż tak. Nie wchodząc w szczegóły, które są objęte tajemnicą. Oczywiście można, należy uzyskane informacje, dowody, opisywać. W jaki sposób, et cetera, zostały uzyskane.

Dam prosty przykład. Jeżeli ja jestem terrorystą, a pani pułkownikiem, pułkownikiem, generałem, jakimkolwiek oficerem kontrwywiadu i pani uzyskała zgodę na podsłuch moich telefonów - jest zgoda w aktach sprawy od do, numer, abonent, imię, nazwisko, figurant rozpracowywany - i ja w rozmowie użyję komunikatu, który jest zaszyfrowaną informacją, że bombę odpalamy tego i tego dnia, więc pani opisuje, że Grzegorz Reszka użył takiego i takiego hasła w rozmowie telefonicznej z i tak dalej. To są bezpośrednie i pośrednie dowody, jakby pośrednie i bezpośrednie, dowiedzenia się, w jaki sposób, jaką drogą został użyty dowód.

Ale ja nie skończyłem poprzedniej wypowiedzi, dlaczego jestem umiarkowanym realistą i optymistą. Otóż być może dokumenty można sfałszować, dokumenty można zniszczyć, ale pani poseł, ja w 2007 roku przychodząc do Służby Kontrwywiadu Wojskowego rozmawiałem z ludźmi, którzy byli zatrudniani przez pana posła Antoniego Macierewicza, ministra wtedy i proszę mi wierzyć: to jest grupa ludzi, która się przedstawia, jako ludzie najwyższej próby moralnej. My dla nich, przepraszam, ja dla nich byłem taki różowy, bo pełniłem służbę razem z oficerami SB w Urzędzie Ochrony Państwa. Niepewny, liberał jakiś taki.

I proszę mi wierzyć, ci spiżowi ludzie w odpowiednich okolicznościach, gdy normalnie się z nimi rozmawia i się ich normalnie traktuje, nie są skłonni do pójścia do końca za swoimi szefami. Otwierają się. Nie jest to ironia. Nie stosowaliśmy żadnych metod, tortur. Uzyskiwaliśmy informacje w rozmowach przy kawie, przychodzili sami. Nie byli wzywani. Antoni Macierewicz informował publicznie, że ja ścigam funkcjonariuszy, po nocy ściągam. To jest nieprawda.

Więc ja jestem optymistą. Nie da się ukryć w służbie stosowania takiego narzędzia w sposób stuprocentowy. Jeśli się panu Bejdzie, bądź jakiemuś innemu szefowi służby, wydaje, że ukryje stosowanie tego narzędzia przed podległymi funkcjonariuszami to wyprowadzam ich z błędu. Nie ukryją. Wcześniej czy później informacja o tym będzie dostępna. W pełni jakby. Inaczej.

Większe możliwości oczywiście uzyska się wtedy, kiedy osoba, która będzie chciała dojść informacji, będzie miała wpływ na to, co się w tej instytucji dzieje. Czyli po spodziewanym przeze mnie, życzonym sobie zmianie kierownictwa służb. To jest to.

Druga rzecz. Więc ja tu jestem optymistą umiarkowanym i sądzę, że coraz więcej informacji będzie na rynku. Są też pośrednicy, są producenci, są dziennikarze krajowi i zagraniczni. Jest sporo osób zainteresowanych i środowisk zainteresowanych dotarciem do prawdy.

Druga rzecz, to, na co pani zwróciła uwagę - koincydencja w czasie, mianowicie zmiany w kodeksie karnym i powiem tak, w czasie, kiedy dokonywano w Polsce zmian w kodeksie karnym to narzędzie już działało, funkcjonowało. To nie było tak, że ono zostało opracowane i wpuszczone na rynek po zmianach w kodeksie karnym. Może było tak, że panowie wiedzieli już o tym, że takie narzędzie istnieje. W związku z tym bardziej ochoczo przystąpili do zmian w kodeksie karnym.

Aczkolwiek trzeba dodać, że te zmiany w kodeksie karnym one umożliwiają również stosowanie jako dowodów np. materiałów uzyskanych w podsłuchu, ale niedotyczących danej sprawy, bo w starej regulacji było tak, że jeżeli ja stosowałem podsłuch, uzyskałem informacje, ale nie odnoszące się do przestępstwa, które rozpoznawałem, to tamte materiały nie mogły być podstawą do wszczęcia przeze mnie oddzielnej sprawy i traktowane jako dowód w sprawie. Ale ten fakt zmiany w kodeksie karnym i nabycie tego urządzenia. Urządzenie, program, jeśli był nabyty, to był nabyty na przełomie 2017 i 2018 roku i implementowany, a zmiany w kodeksie karnym w 2016.

Według niektórych informatyków, program Pegasus funkcjonuje od co najmniej 2013 roku i jest to już jego któraś wersja. Na jedną z tych pierwszych wersji Apple znalazł antidotum i zastosował dwie lub trzy łatki, ale już funkcjonuje kolejny Pegasus. Tak? Poza tym Pegasus jest w mutacjach na dwa systemy operacyjne. Nie tylko iOS również i Android, więc cały czas pracuje się nad tym.

Pytanie dotyczące USA. Służby USA oczywiście są też służbami partnerskimi wobec naszych służb. O wspólnej pracy oczywiście nic nie mogę powiedzieć. Natomiast ja wypowiadałem tutaj taką opinię, co do tego, by zadać sobie trud i dokładnie zbadać strukturę własności, bo jeszcze raz powiem, w opinii, w obiegu publicznym jest informacja, że program Pegasus jest autorstwa byłych oficerów Mosadu, a spółka NSO jest spółką izraelską. Ja natomiast natrafiłem

na informację taką, jak mówiłem. W ciągu 30, 40 sekund szukania w wyszukiwarce internetowej trafiłem na informacje, że spółka NSO jest własnością amerykańskiej spółki, więc wydaje się jest wiele tropów, którymi trzeba pójść i którymi w sposób stosunkowo łatwy można pójść i uzyskać informacje, ale nie sądzę, żeby za obecnej administracji polskiej.

Nie sądzę, by pan premier Morawiecki zechciał tutaj wyczerpać pełną drogę w poinformowaniu opinii publicznej w prostej sprawie. Czy ma takie narzędzie, czy nie ma takich narzędzi służba? A jeśli ma, to dlaczego zostało kupione? Jakie motywy były przy nabyciu tego narzędzia skoro ma wystarczające możliwości techniczne i prawne, by uzyskiwać informacje z podsłuchu? Wszystko. Maile, sms-y, rozmowy telefoniczne. Wszystko. Z wyłączeniem szyfrowanych komunikatorów.

I jeszcze jedna rzecz. Bo to też nie dość dobrze wybrzmiało. Wszystkich nas dziwi, że potencjalnym, ewentualnym nabywcą tego sprzętu jest CBA. Jest mi łatwo wyobrazić sobie taką sytuację. Gdyby tak cwanie chcieli zrobić, to nie kazaliby kupować CBA tego sprzętu, tego programu, bo to się rzuca w oczy, bo to od razu dziwi.

Dlaczego nie ABW? Dlaczego nie SKW? Odpowiedź może być banalnie prosta. Może polegać na tym, że być może szefowie ABW albo SKW wyrazili obawy, lęk. Po prostu strach, a proszę mi wierzyć nie traktujmy wszystkich funkcjonariuszy PIS-u, wszystkich osób pełniących wysokie funkcje państwowe jako śpiżowych, nieugiętych jak pan prezydent Andrzej Duda mówił o sobie, że jest niezłomny.

Nie traktujmy wszystkich jako takich, którzy nie mają wątpliwości moralnych. Są tacy, którzy mają wątpliwości moralne i naprawdę nie mówię tego w oparciu o czystą teorię, mówię w oparciu o praktykę. Ja mam kilku kolegów. Nie wymienię ich nazwisk, no bo w sposób oczywisty byliby zniszczeni po tamtej stronie. Mam kilka osób z PIS- u, które pełniły, bądź pełnią funkcje w służbach, z którymi się spotykamy regularnie na kawie. Warunek taki, żeby nie nagłaśniać naszej znajomości, no bo to im zaszkodzi. Pegasus wejdzie i sprawę załatwi.

Więc z tym CBA może być tak, że rzeczywiście to wygląda jak łapanie się prawą ręką za lewe ucho, do czego też nas przyzwyczaił rząd PiS-owski. Także proste rzeczy w sposób kuriozalny i karykaturalny, ale mogło być i tak, że na propozycje zakupu takiego sprzętu za tyle milionów złotych jeden i drugi szef powiedział: nie, przepraszam nie. Dziękuje to jest ryzykowne.

No, ale CBA to jest kierownictwo. Kierownictwo CBA to jest kierownictwo crème de la crème, to są ci może niezłomni, którzy nie mieli wątpliwości moralnych ani prawnych.

Więc ja generalnie upieram się w rokowaniach na przyszłość, na umiarkowanym optymizmie polegającym na tym: ani dziennikarze, ani opinia publiczna, ani opozycja nie odpuści. A po drugie, będą narastać wątpliwości wśród tych, którzy używają tego sprzętu. Bo oni muszą mieć świadomość, że robią to nielegalnie. Oni wiedzą po prostu, że nielegalnie podsłuchują, a robiąc to, łamią prawo. Ktoś kiedyś może przyjść i powiedzieć zwalniam cię nie dlatego, że byłeś nominatem PIS- u, zwalniam cię dlatego, że masz postawione zarzuty kodeksu karnego. Ta przestroga musi im brzmieć w uszach, że robią coś nielegalnie, że łamią prawo.

Joanna Kluzik-Rostkowska, przewodnicząca zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Dziękuję panie pułkowniku.

Podsumowując. Będziemy domagać się wyjaśnień od pana premiera Morawieckiego. Chcemy mu zadać te wszystkie pytania, które pan tutaj przed chwilą przedstawił, czyli, czy miał świadomość do czego to służyło i do czego potrzebne są nielegalne instrumenty, skoro legalne instrumenty istnieją? Brak odpowiedzi na pytanie, czy ten system został kupiony, czy też takie milczenie władz, każe nam się domyślać tylko, że ten system istnieje i funkcjonuje właśnie i służy po to, żebyśmy mogli być nielegalnie podsłuchiwani.

Żeby była jasność, każdy użytkownik takiego telefonu, nie tylko, kiedy jest politykiem opozycji, czy też partii rządzącej, bo nie sadzę, żeby byli bezpieczni, tylko wtedy, kiedy dziennikarzem, ale też wtedy, kiedy jest przedsiębiorcą, budowlańcem, nauczycielem itd.

Przypomnijmy sobie, ile emocji budziła afera podsłuchowa w latach 2014-2015, po prostu nagrania. Ile emocji budzi afera podkarpacka, czyli mowa o tym, że istnieje 4 tysiące nagrań. Ile emocji budzą te informacje, które docierają do nas z Ministerstwa Sprawiedliwości, czyli takiego zinstytucjonalizowanego hejtu przy użyciu formacji wrażliwych czy też danych wrażliwych. Pojawiają się znaki zapytania dotyczące tego, czy ten hejt był skierowany wyłącznie do środowiska sprawiedliwości, czy nie był również używany w przypadku nauczycieli, czy innych grup zawodowych, które podpadły.

No i wyobraźmy sobie, że te wszystkie narzędzia, których używał PIS w przeszłości, były absolutnie niedoskonałe w porównaniu z tym Pegasusem, który ma dostęp nie tylko taki bierny do, co mamy w telefonach, ale do tego, co może nas nagrywać, robić nam zdjęcia, grzebać w naszej korespondencji. Robi to absolutnie nielegalnie, ale, co ważne, z punktu widzenia tych, co na ten system się zdecydowali, robi to właściwie bez śladu.

Więc proszę państwa, wszyscy ci, którzy do tej pory myśleli, że jakoś w państwie PIS dadzą radę i mogą czuć się bezpiecznie, nie. Jeżeli jesteście posiadaczami telefonu komórkowego, czymkolwiek się zajmujecie w życiu, nie jesteście bezpieczni.

Uważam, że sprawa jest tak ważna nie tylko z punktu widzenia ochrony interesów poszczególnych obywateli, ale właśnie zagrożeń bezpieczeństwa państwa. Tym się zajmujemy tutaj w zespole od dwóch lat. Absolutnie będziemy się domagać jednoznacznych wyjaśnień od premiera i wcześniej czy później będzie musiał na to pytanie odpowiedzieć. Nie ucieknie od tego pytania i odpowiedzialności, jeżeli rzeczywiście ten Pegasus jest faktem.

Dorota Niedziela, członek zespołu śledczego Platformy Obywatelskiej ds. zagrożeń bezpieczeństwa państwa: Ja jeszcze bym zwróciła uwagę na to, co usłyszeliśmy a mianowicie to ogromne niebezpieczeństwo dla państwa, czyli ten koń trojański, który jest wpuszczony, czyli taka obusieczna broń, która może spowodować, że ważne informacje państwowe będą mogły wypływać do obcych wywiadów.

Płk Grzegorz Reszka, były zastępca szefa UOP, w latach 2007-2008 pełnił obowiązki szefa SKW: Dokładnie tak. Jeśli takie możliwości techniczne ten program ma, o jakich mówiłem, a one pojawiły się w wypowiedzi jednego z pracowników spółki NSO, to nie jest mój wymysł, to jest cytat z wypowiedzi jednego z pracowników spółki NSO, który powiedział, że spółka ma możliwości audytowania na odległość.

Jeśli tak, to znaczy gospodarzem uzyskanych informacji, już pomińmy nielegalnych, w nielegalny sposób itd., jest nie tylko służba, polska służba, która użytkuje, ale producent, bądź przyjaciel producenta. Nie wiadomo, kto może to audytować na odległość. Wiemy doskonale, że na tym polega specyfika urządzeń, programów komputerowych, że w sposób zdalny on-line można wykonywać pewne czynności, przestrzeń geograficzna, odległość geograficzna, nie jest tu istotna. Nie jest przeszkodą.

Problem jest naprawdę duży i nie sądzę, by użytkownicy polscy ewentualni tego programu zdawali sobie z tego sprawę. Jeśli nie zdają sobie sprawy, to powinni zacząć przynajmniej minimalizować straty, które mogą wyniknąć z użytkowania tego programu. Mówię tak, bo prawdopodobieństwo nabycia tego programu przez polskie służby jest wysokie.

I jeszcze jedną uwagę chciałbym dodać. Fakt, że nabyła ten program ewentualnie CBA, biorąc pod uwagę tryb działania służb, wcale nie stoi w przeszkodzie przed używaniem tego programu przez inne służby. Proszę pamiętać, że jest to w ogóle poza jakimkolwiek prawem. W związku z tym użytkowanie tego programu, ono polega na tym, że się wykupuje określoną liczbę licencji, czyli numerów telefonów, operacji, na które się …numerów telefonów, na które się można zalogować i wejść wysyłając wirusy. To nie jest przeszkodą. Jeżeli panowie szefowie pod kierownictwem ministra Kamińskiego uznają, że proszę bardzo, możemy, to proszę bardzo możemy. Jest to poza trybem. Poza prawem. Nie ma nad tym nikt kontroli.

Joanna Kluzik-Rostkowska: Dziękujemy panie pułkowniku bardzo. Zamykam posiedzenie.